CVE Name	Description	Severity
CVE-2020-9724	Adobe Lightroom versions 9.2.0.10 and earlier have an insecure library loading vulnerability. Successful exploitation could lead to privilege escalation. **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.8 HIGH V2.0: 6.8 MEDIUM
CVE-2020-9723	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-9722	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.8 HIGH V2.0: 9.3 HIGH
CVE-2020-9721	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-9720	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-9719	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-9718	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-9717	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-9716	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 11:15:13 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-9715	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 10:15:13 AM -0400	V3.1: 7.8 HIGH V2.0: 9.3 HIGH
CVE-2020-9714	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation . **Published:** August 19, 2020; 10:15:13 AM -0400	V3.1: 7.8 HIGH V2.0: 6.8 MEDIUM

CVE-2020-9712	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **Published:** August 19, 2020; 10:15:13 AM -0400	V3.1: 5.5 MEDIUM V2.0: 7.1 HIGH
CVE-2020-9710	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 10:15:13 AM -0400	V3.1: 3.3 LOW V2.0: 4.3 MEDIUM
CVE-2020-9707	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 3.3 LOW V2.0: 4.3 MEDIUM
CVE-2020-9706	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 3.3 LOW V2.0: 4.3 MEDIUM
CVE-2020-9705	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-9704	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 7.8 HIGH V2.0: 9.3 HIGH
CVE-2020-9703	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 5.5 MEDIUM V2.0: 4.3 MEDIUM
CVE-2020-9702	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 5.5 MEDIUM V2.0: 4.3 MEDIUM
CVE-2020-9697	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a disclosure of sensitive data vulnerability. Successful exploitation could lead to memory leak. **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 5.5 MEDIUM V2.0: 4.3 MEDIUM
CVE-2020-9696	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 5.5 MEDIUM V2.0: 7.1 HIGH
CVE-2020-9694	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 7.8 HIGH V2.0: 6.8 MEDIUM

CVE-2020-9693	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 10:15:12 AM -0400	V3.1: 7.8 HIGH V2.0: 9.3 HIGH
CVE-2020-9701	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 9:15:10 AM -0400	V3.1: 7.8 HIGH V2.0: 9.3 HIGH
CVE-2020-9700	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 9:15:10 AM -0400	V3.1: 7.8 HIGH V2.0: 9.3 HIGH
CVE-2020-9699	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 9:15:10 AM -0400	V3.1: 7.8 HIGH V2.0: 9.3 HIGH
CVE-2020-9698	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **Published:** August 19, 2020; 9:15:10 AM -0400	V3.1: 7.8 HIGH V2.0: 9.3 HIGH
CVE-2020-15926	Rocket.Chat through 3.4.2 allows XSS where an attacker can send a specially crafted message to a channel or in a direct message to the client which results in remote code execution on the client side. **Published:** August 18, 2020; 5:15:12 PM -0400	V3.1: 6.1 MEDIUM V2.0: 4.3 MEDIUM
CVE-2020-1554	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525. **Published:** August 17, 2020; 3:15:19 PM -0400	V3.1: 7.8 HIGH V2.0: 6.8 MEDIUM
CVE-2020-1551	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547. **Published:** August 17, 2020; 3:15:19 PM -0400	V3.1: 7.8 HIGH V2.0: 4.6 MEDIUM
CVE-2020-1546	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1547, CVE-2020-1551. **Published:** August 17, 2020; 3:15:19 PM -0400	V3.1: 7.8 HIGH V2.0: 4.6 MEDIUM
CVE-2020-1545	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **Published:** August 17, 2020; 3:15:19 PM -0400	V3.1: 7.8 HIGH V2.0: 4.6 MEDIUM

CVE-2020-1544	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	V3.1: 7.8 HIGH V2.0: 4.6 MEDIUM
	Published: August 17, 2020; 3:15:19 PM -0400	
CVE-2020-1543	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	V3.1: 7.8 HIGH V2.0: 4.6 MEDIUM
	Published: August 17, 2020; 3:15:19 PM -0400	
CVE-2020-1542	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:19 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1541	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:18 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1540	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:18 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1539	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:18 PM -0400	V2.0: 4.6 ME
CVE-2020-1536	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:18 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1525	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory	V3.1: 8.8 HIGH

	Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1554.	
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 6.8 MEDIUM
CVE-2020-1522	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1521.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1521	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1522.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1520	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 7.2 HIGH
CVE-2020-1519	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1538.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1518	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1517	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1516	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1515	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1513	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM

CVE-2020-1512	An information disclosure vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Information Disclosure Vulnerability'.	V3.1: 5.5 MEDIUM
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.3 MEDIUM
CVE-2020-1511	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-1510	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	V3.1: 5.5 MEDIUM
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 4.3 MEDIUM
CVE-2020-1509	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'.	V3.1: 8.8 HIGH
	Published: August 17, 2020; 3:15:17 PM -0400	V2.0: 6.5 MEDIUM
CVE-2020-1379	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:14 PM -0400	V2.0: 6.8 MEDIUM
CVE-2020-1378	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:14 PM -0400	V2.0: 7.2 HIGH
CVE-2020-1377	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1378.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 3:15:14 PM -0400	V2.0: 7.2 HIGH
CVE-2020-1339	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'.	V3.1: 8.8 HIGH V2.0: 9.3 HIGH
	Published: August 17, 2020; 3:15:14 PM -0400	
CVE-2020-3502	Multiple vulnerabilities in the user interface of Cisco Webex Meetings Desktop App could allow an authenticated, remote attacker to obtain restricted information from other Webex users. These vulnerabilities are due to improper input validation of parameters returned to the application from a web site. An attacker with a valid Webex account could exploit these vulnerabilities by persuading a user to follow a URL that is designed to return malicious path parameters to the affected software. A successful exploit could allow the attacker to obtain restricted information from other Webex users.	V3.1: 4.1 MEDIUM
	Published: August 17, 2020; 2:15:14 PM -0400	V2.0: 3.5 LOW
CVE-2020-3501	Multiple vulnerabilities in the user interface of Cisco Webex Meetings Desktop App could allow an authenticated, remote attacker to obtain restricted information from other Webex users. These vulnerabilities are due to improper input validation of parameters returned to the application from a web site. An attacker with a valid Webex account could exploit these vulnerabilities by persuading a user to follow a URL that is designed to return malicious path parameters to the affected software. A successful exploit could allow the attacker to obtain restricted information from other Webex users.	V3.1: 4.1 MEDIUM
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 3.5 LOW

CVE-2020-3500	A vulnerability in the IPv6 implementation of Cisco StarOS could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet to an affected device with the goal of reaching the vulnerable section of the input buffer. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	V3.1: 8.6 HIGH
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 7.8 HIGH
CVE-2020-3472	A vulnerability in the contacts feature of Cisco Webex Meetings could allow an authenticated, remote attacker with a legitimate user account to access sensitive information. The vulnerability is due to improper access restrictions on users who are added within user contacts. An attacker on one Webex Meetings site could exploit this vulnerability by sending specially crafted requests to the Webex Meetings site. A successful exploit could allow the attacker to view the details of users on another Webex site, including user names and email addresses.	V3.1: 5.0 MEDIUM
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 4.0 MEDIUM
CVE-2020-3464	A vulnerability in the web-based management interface of Cisco UCS Director could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker would need administrative credentials on the affected device.	V3.1: 4.8 MEDIUM
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 3.5 LOW
CVE-2020-3463	A vulnerability in the web-based management interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected service. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected service. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	V3.1: 6.1 MEDIUM
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 4.3 MEDIUM
CVE-2020-3449	A vulnerability in the Border Gateway Protocol (BGP) additional paths feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to prevent authorized users from monitoring the BGP status and cause the BGP process to stop processing new updates, resulting in a denial of service (DOS) condition. The vulnerability is due to an incorrect calculation of lexicographical order when displaying additional path information within Cisco IOS XR Software, which causes an infinite loop. An attacker could exploit this vulnerability by sending a specific BGP update from a BGP neighbor peer session of an affected device; an authorized user must then issue a show bgp command for the vulnerability to be exploited. A successful exploit could allow the attacker to prevent authorized users from properly monitoring the BGP status and prevent BGP from processing new updates, resulting in outdated information in the routing and forwarding tables.	V3.1: 4.3 MEDIUM
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 4.3 MEDIUM
CVE-2020-3448	A vulnerability in an access control mechanism of Cisco Cyber Vision Center Software could allow an unauthenticated, remote attacker to bypass authentication and access internal services that are running on an affected device. The vulnerability is due to insufficient enforcement of access control in the software. An attacker could exploit this vulnerability by directly accessing the internal services of an affected device. A successful exploit	V3.1: 5.8 MEDIUM

	could allow an attacker to impact monitoring of sensors that are managed by the software.	
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-3447	A vulnerability in the CLI of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco AsyncOS for Cisco Content Security Management Appliance (SMA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to excessive verbosity in certain log subscriptions. An attacker could exploit this vulnerability by accessing specific log files on an affected device. A successful exploit could allow the attacker to obtain sensitive log data, which may include user credentials. To exploit this vulnerability, the attacker would need to have valid credentials at the operator level or higher on the affected device.	V3.1: 6.5 MEDIUM
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 4.0 MEDIUM
CVE-2020-3435	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to overwrite VPN profiles on an affected device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process on an affected device. A successful exploit could allow the attacker to modify VPN profile files. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.	V3.1: 5.5 MEDIUM
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 2.1 LOW
CVE-2020-3434	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process on an affected device. A successful exploit could allow the attacker to stop the AnyConnect process, causing a DoS condition on the device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.	V3.1: 5.5 MEDIUM
	Published: August 17, 2020; 2:15:13 PM -0400	V2.0: 4.9 MEDIUM
CVE-2020-3433	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.	V3.1: 7.8 HIGH
	Published: August 17, 2020; 2:15:12 PM -0400	V2.0: 7.2 HIGH
CVE-2020-7704	The package linux-cmdline before 1.0.1 are vulnerable to Prototype Pollution via the constructor.	V3.1: 9.8 CRITICAL
	Published: August 17, 2020; 1:15:14 PM -0400	V2.0: 7.5 HIGH
CVE-2020-24208	A SQL injection vulnerability in SourceCodester Online Shopping Alphaware 1.0 allows remote unauthenticated attackers to bypass the authentication process via email and password parameters.	V3.1: 9.8 CRITICAL

	Published: August 17, 2020; 1:15:13 PM -0400	V2.0: 7.5 HIGH
CVE-2020-9241	Huawei 5G Mobile WiFi E6878-370 with versions of 10.0.3.1(H563SP1C00),10.0.3.1(H563SP21C233) have an improper authorization vulnerability. The device does not restrict certain data received from WAN port. Successful exploit could allow an attacker at WAN side to manage certain service of the device.	V3.1: 7.0 HIGH
	Published: August 17, 2020; 12:15:14 PM -0400	V2.0: 6.8 MEDIUM
CVE-2020-9237	Huawei smartphone Taurus-AL00B with versions earlier than 10.1.0.126(C00E125R5P3) have a user after free vulnerability. A module is lack of lock protection. Attackers can exploit this vulnerability by launching specific request. This could compromise normal service of the affected device.	V3.1: 6.7 MEDIUM
	Published: August 17, 2020; 12:15:14 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-9233	FusionCompute 8.0.0 have an insufficient authentication vulnerability. An attacker may exploit the vulnerability to delete some files and cause some services abnormal.	V3.1: 9.1 CRITICAL
	Published: August 17, 2020; 12:15:13 PM -0400	V2.0: 6.4 MEDIUM
CVE-2020-8233	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges.	V3.1: 8.8 HIGH
	Published: August 17, 2020; 12:15:13 PM -0400	V2.0: 9.0 HIGH
CVE-2020-8232	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages.	V3.1: 6.5 MEDIUM
	Published: August 17, 2020; 12:15:13 PM -0400	V2.0: 4.0 MEDIUM
CVE-2020-8230	A memory corruption vulnerability exists in NextCloud Desktop Client v2.6.4 where missing ASLR and DEP protections in for windows allowed to corrupt memory.	V3.1: 5.5 MEDIUM
	Published: August 17, 2020; 12:15:13 PM -0400	V2.0: 2.1 LOW
CVE-2020-8226	A vulnerability exists in phpBB <v3.2.10 and <v3.3.1 which allowed remote image dimensions check to be used to SSRF.	V3.1: 5.8 MEDIUM
	Published: August 17, 2020; 12:15:13 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-8212	Improper access control in Citrix XenMobile Server 10.12 before RP3, Citrix XenMobile Server 10.11 before RP6, Citrix XenMobile Server 10.10 RP6 and Citrix XenMobile Server before 10.9 RP5 allows access to privileged functionality.	V3.1: 9.8 CRITICAL
	Published: August 17, 2020; 12:15:13 PM -0400	V2.0: 7.5 HIGH
CVE-2020-8683	Improper buffer restrictions in system driver for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable denial of service via local access.	V3.1: 5.5 MEDIUM
	Published: August 13, 2020; 12:15:13 AM -0400	V2.0: 2.1 LOW
CVE-2020-8682	Out of bounds read in system driver for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable denial of service via local access.	V3.1: 5.5 MEDIUM
	Published: August 13, 2020; 12:15:13 AM -0400	V2.0: 2.1 LOW
CVE-2020-8681	Out of bounds write in system driver for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable escalation of privilege via local access.	V3.1: 7.8 HIGH
	Published: August 13, 2020; 12:15:13 AM -0400	V2.0: 4.6 MEDIUM
CVE-2020-8680	Race condition in some Intel(R) Graphics Drivers before version 15.40.45.5126 may allow an authenticated user to potentially enable escalation of privilege via local access.	V3.1: 7.0 HIGH
	Published: August 13, 2020; 12:15:13 AM -0400	V2.0: 4.4 MEDIUM
CVE-2020-8679	Out-of-bounds write in Kernel Mode Driver for some Intel(R) Graphics Drivers before version 26.20.100.7755 may allow an authenticated user to potentially enable denial of service via local access.	V3.1: 5.5 MEDIUM
	Published: August 13, 2020; 12:15:13 AM -0400	V2.0: 2.1 LOW

CVE-2020-7307	Unprotected Storage of Credentials vulnerability in McAfee Data Loss Prevention (DLP) for Mac prior to 11.5.2 allows local users to gain access to the RiskDB username and password via unprotected log files containing plain text credentials.	V3.1: 5.2 MEDIUM
	Published: August 13, 2020; 12:15:13 AM -0400	V2.0: 2.1 LOW
CVE-2020-12301	Improper initialization in BIOS firmware for Intel(R) Server Board Families S2600ST, S2600BP and S2600WF may allow a privileged user to potentially enable escalation of privilege via local access.	V3.1: 8.2 HIGH
	Published: August 13, 2020; 12:15:13 AM -0400	V2.0: 4.6 MEDIUM
CVE-2020-12300	Uninitialized pointer in BIOS firmware for Intel(R) Server Board Families S2600CW, S2600KP, S2600TP, and S2600WT may allow a privileged user to potentially enable escalation of privilege via local access.	V3.1: 8.2 HIGH
	Published: August 13, 2020; 12:15:13 AM -0400	V2.0: 4.6 MEDIUM
CVE-2020-12299	Improper input validation in BIOS firmware for Intel(R) Server Board Families S2600ST, S2600BP and S2600WF may allow a privileged user to potentially enable escalation of privilege via local access.	V3.1: 8.2 HIGH
	Published: August 13, 2020; 12:15:12 AM -0400	V2.0: 4.6 MEDIUM
CVE-2020-0559	Insecure inherited permissions in some Intel(R) PROSet/Wireless WiFi products on Windows* 7 and 8.1 before version 21.40.5.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	V3.1: 7.8 HIGH
	Published: August 13, 2020; 12:15:12 AM -0400	V2.0: 4.6 MEDIUM
CVE-2020-0555	Improper input validation for some Intel(R) Wireless Bluetooth(R) products may allow an authenticated user to potentially enable escalation of privilege via local access.	V3.1: 7.8 HIGH
	Published: August 13, 2020; 12:15:12 AM -0400	V2.0: 4.6 MEDIUM
CVE-2020-0554	Race condition in software installer for some Intel(R) Wireless Bluetooth(R) products on Windows* 7, 8.1 and 10 may allow an unprivileged user to potentially enable escalation of privilege via local access.	V3.1: 7.0 HIGH
	Published: August 13, 2020; 12:15:12 AM -0400	V2.0: 3.7 LOW
CVE-2020-0553	Out-of-bounds read in kernel mode driver for some Intel(R) Wireless Bluetooth(R) products on Windows* 10, may allow a privileged user to potentially enable information disclosure via local access.	V3.1: 4.4 MEDIUM
	Published: August 13, 2020; 12:15:12 AM -0400	V2.0: 2.1 LOW
CVE-2020-0513	Out of bounds write for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable escalation of privilege via local access.	V3.1: 7.8 HIGH
	Published: August 13, 2020; 12:15:12 AM -0400	V2.0: 4.6 MEDIUM
CVE-2020-0512	Uncaught exception in the system driver for some Intel(R) Graphics Drivers before version 15.33.50.5129 may allow an authenticated user to potentially enable denial of service via local access.	V3.1: 5.5 MEDIUM
	Published: August 13, 2020; 12:15:12 AM -0400	V2.0: 2.1 LOW
CVE-2020-0510	Out of bounds read in some Intel(R) Graphics Drivers before versions 15.45.31.5127 and 15.40.45.5126 may allow an authenticated user to potentially enable escalation of privilege via local access.	V3.1: 7.8 HIGH
	Published: August 13, 2020; 12:15:12 AM -0400	V2.0: 4.6 MEDIUM
CVE-2020-17446	asyncpg before 0.21.0 allows a malicious PostgreSQL server to trigger a crash or execute arbitrary code (on a database client) via a crafted server response, because of access to an uninitialized pointer in the array data decoder.	V3.1: 9.8 CRITICAL
	Published: August 12, 2020; 12:15:11 PM -0400	V2.0: 7.5 HIGH
CVE-2020-0241	In NuPlayerStreamListener of NuPlayerStreamListener.cpp, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-151456667	V3.1: 7.8 HIGH
	Published: August 11, 2020; 4:15:12 PM -0400	V2.0: 7.2 HIGH

CVE-2020-0240	In NewFixedDoubleArray of factory.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-150706594	V3.1: 8.8 HIGH
	Published: August 11, 2020; 4:15:12 PM -0400	V2.0: 9.3 HIGH
CVE-2020-0239	In getDocumentMetadata of DocumentsContract.java, there is a possible disclosure of location metadata from a file due to a permissions bypass. This could lead to local information disclosure from a file (eg. a photo) containing location metadata with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-151095863	V3.1: 5.5 MEDIUM
	Published: August 11, 2020; 4:15:12 PM -0400	V2.0: 4.9 MEDIUM
CVE-2020-0238	In updatePreferenceIntents of AccountTypePreferenceLoader, there is a possible confused deputy attack due to a race condition. This could lead to local escalation of privilege and launching privileged activities with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-150946634	V3.1: 7.0 HIGH
	Published: August 11, 2020; 4:15:11 PM -0400	V2.0: 6.9 MEDIUM
CVE-2020-0108	In postNotification of ServiceRecord.java, there is a possible bypass of foreground process restrictions due to an uncaught exception. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-140108616	V3.1: 7.8 HIGH
	Published: August 11, 2020; 4:15:11 PM -0400	V2.0: 7.2 HIGH
CVE-2019-17339	The VirtualRouter component of TIBCO Software Inc.'s TIBCO Silver Fabric contains a vulnerability that theoretically allows an attacker to inject scripts via URLs. The attacker could theoretically social engineer an authenticated user into submitting the URL, thus executing the script on the affected system with the privileges of the user. Affected releases are TIBCO Software Inc.'s TIBCO Silver Fabric: versions 6.0.0 and below.	V3.1: 8.1 HIGH
	Published: August 11, 2020; 4:15:11 PM -0400	V2.0: 5.8 MEDIUM
CVE-2020-9404	In PACTware before 4.1 SP6 and 5.x before 5.0.5.31, passwords are stored in an insecure manner, and may be modified by an attacker with no knowledge of the current passwords.	V3.1: 7.1 HIGH
	Published: August 11, 2020; 3:15:17 PM -0400	V2.0: 3.6 LOW
CVE-2020-9403	In PACTware before 4.1 SP6 and 5.x before 5.0.5.31, passwords are stored in a recoverable format, and may be retrieved by any user with access to the PACTware workstation.	V3.1: 5.5 MEDIUM
	Published: August 11, 2020; 3:15:17 PM -0400	V2.0: 2.1 LOW
CVE-2020-9244	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5),Versions earlier than 10.1.0.270(C635E3R1P5),Versions earlier than 10.1.0.273(C636E7R2P4);HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged	V3.1: 6.8 MEDIUM
	Published: August 11, 2020; 3:15:17 PM -0400	V2.0: 4.6 MEDIUM

CVE-2020-8918	An improperly initialized 'migrationAuth' value in Google's go-tpm TPM1.2 library versions prior to 0.3.0 can lead an eavesdropping attacker to discover the auth value for a key created with CreateWrapKey. An attacker listening in on the channel can collect both 'encUsageAuth' and 'encMigrationAuth', and then can calculate 'usageAuth ^ encMigrationAuth' as the 'migrationAuth' can be guessed for all keys created with CreateWrapKey. TPM2.0 is not impacted by this. We recommend updating your library to 0.3.0 or later, or, if you cannot update, to call CreateWrapKey with a random 20-byte value for 'migrationAuth'.	V3.1: 7.1 HIGH
	Published: August 11, 2020; 3:15:17 PM -0400	V2.0: 3.6 LOW
CVE-2020-13179	Broker Protocol messages in Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows prior to 20.04.1 are not cleaned up in server memory, which may allow an attacker to read confidential information from a memory dump via forcing a crashing during the single sign-on procedure.	V3.1: 5.5 MEDIUM
	Published: August 11, 2020; 3:15:17 PM -0400	V2.0: 2.1 LOW
CVE-2020-11976	By crafting a special URL it is possible to make Wicket deliver unprocessed HTML templates. This would allow an attacker to see possibly sensitive information inside a HTML template that is usually removed during rendering. Affected are Apache Wicket versions 7.16.0, 8.8.0 and 9.0.0-M5	V3.1: 7.5 HIGH
	Published: August 11, 2020; 3:15:17 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-15071	content/content.blueprintsevents.php in Symphony CMS 3.0.0 allows XSS via fields['name'] to appendSubheading.	V3.1: 6.1 MEDIUM
	Published: August 11, 2020; 2:15:13 PM -0400	V2.0: 4.3 MEDIUM
CVE-2020-14979	The WinRing0.sys and WinRing0x64.sys drivers 1.2.0 in EVGA Precision X1 through 1.0.6 allow local users, including low integrity processes, to read and write to arbitrary memory locations. This allows any user to gain NT AUTHORITY\SYSTEM privileges by mapping \Device\PhysicalMemory into the calling process.	V3.1: 7.8 HIGH
	Published: August 11, 2020; 2:15:12 PM -0400	V2.0: 7.2 HIGH
CVE-2020-13178	A function in the Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows prior to version 20.04.1 does not properly validate the signature of an external binary, which could allow an attacker to gain elevated privileges via execution in the context of the PCoIP Agent process.	V3.1: 6.7 MEDIUM
	Published: August 11, 2020; 2:15:12 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-13177	The support bundler in Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows versions prior to 20.04.1 and 20.07.0 does not use hard coded paths for certain Windows binaries, which allows an attacker to gain elevated privileges via execution of a malicious binary placed in the system path.	V3.1: 7.8 HIGH
	Published: August 11, 2020; 2:15:12 PM -0400	V2.0: 4.4 MEDIUM
CVE-2020-13176	The Management Interface of the Teradici Cloud Access Connector and Cloud Access Connector Legacy for releases prior to April 24, 2020 (v16 and earlier for the Cloud Access Connector) contains a stored cross-site scripting (XSS) vulnerability which allows a remote unauthenticated attacker to poison log files with malicious JavaScript via the login page which is executed when an administrator views the logs within the application.	V3.1: 6.1 MEDIUM
	Published: August 11, 2020; 2:15:12 PM -0400	V2.0: 4.3 MEDIUM
CVE-2020-13175	The Management Interface of the Teradici Cloud Access Connector and Cloud Access Connector Legacy for releases prior to April 20, 2020 (v15 and earlier for Cloud Access Connector) contains a local file inclusion vulnerability which allows an unauthenticated remote attacker to leak LDAP credentials via a specially crafted HTTP request.	V3.1: 7.5 HIGH
	Published: August 11, 2020; 2:15:12 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-13174	The web server in the Teradici Managament console versions 20.04 and 20.01.1 did not properly set the X-Frame-Options HTTP header, which could allow an attacker to trick a user into clicking a malicious link via clickjacking.	V3.1: 6.1 MEDIUM
	Published: August 11, 2020; 2:15:12 PM -0400	V2.0: 4.3 MEDIUM

CVE-2020-17466	Turcom TRCwifiZone through 2020-08-10 allows authentication bypass by visiting manage/control.php and ignoring 302 Redirect responses.	V3.1: 9.8 CRITICAL
	Published: August 11, 2020; 1:15:12 PM -0400	V2.0: 7.5 HIGH
CVE-2020-17448	Telegram Desktop through 2.1.13 allows a spoofed file type to bypass the Dangerous File Type Execution protection mechanism, as demonstrated by use of the chat window with a filename that lacks an extension.	V3.1: 7.8 HIGH
	Published: August 11, 2020; 1:15:12 PM -0400	V2.0: 6.8 MEDIUM
CVE-2020-17368	Firejail through 0.9.62 mishandles shell metacharacters during use of the --output or --output-stderr option, which may lead to command injection.	V3.1: 9.8 CRITICAL
	Published: August 11, 2020; 12:15:12 PM -0400	V2.0: 7.5 HIGH
CVE-2020-17367	Firejail through 0.9.62 does not honor the -- end-of-options indicator after the --output option, which may lead to command injection.	V3.1: 7.8 HIGH
	Published: August 11, 2020; 12:15:12 PM -0400	V2.0: 4.6 MEDIUM
CVE-2020-16092	In QEMU through 5.0.0, an assertion failure can occur in the network packet processing. This issue affects the e1000e and vmxnet3 network devices. A malicious guest user/process could use this flaw to abort the QEMU process on the host, resulting in a denial of service condition in net_tx_pkt_add_raw_fragment in hw/net/net_tx_pkt.c.	V3.1: 7.5 HIGH
	Published: August 11, 2020; 12:15:12 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-15597	SOPlanning 1.46.01 allows persistent XSS via the Project Name, Statutes Comment, Places Comment, or Resources Comment field.	V3.1: 5.4 MEDIUM
	Published: August 11, 2020; 12:15:12 PM -0400	V2.0: 3.5 LOW
CVE-2020-13124	SABnzbd 2.3.9 and 3.0.0Alpha2 has a command injection vulnerability in the web configuration interface that permits an authenticated user to execute arbitrary Python commands on the underlying operating system.	V3.1: 8.8 HIGH
	Published: August 11, 2020; 12:15:12 PM -0400	V2.0: 6.5 MEDIUM
CVE-2020-11552	An elevation of privilege vulnerability exists in ManageEngine ADSelfService Plus before build 6003 because it does not properly enforce user privileges associated with a Certificate dialog. This vulnerability could allow an unauthenticated attacker to escalate privileges on a Windows host. An attacker does not require any privilege on the target system in order to exploit this vulnerability. One option is the self-service option on the Windows login screen. Upon selecting this option, the thick-client software is launched, which connects to a remote ADSelfService Plus server to facilitate self-service operations. An unauthenticated attacker having physical access to the host could trigger a security alert by supplying a self-signed SSL certificate to the client. The View Certificate option from the security alert allows an attacker to export a displayed certificate to a file. This can further cascade to a dialog that can open Explorer as SYSTEM. By navigating from Explorer to \windows\system32, cmd.exe can be launched as a SYSTEM.	V3.1: 9.8 CRITICAL
	Published: August 11, 2020; 12:15:12 PM -0400	V2.0: 10.0 HIGH
CVE-2020-14324	A high severity vulnerability was found in all active versions of Red Hat CloudForms before 5.11.7.0. The out of band OS command injection vulnerability can be exploited by authenticated attacker while setuping conversion host through Infrastructure Migration Solution. This flaw allows attacker to execute arbitrary commands on CloudForms server.	V3.1: 9.1 CRITICAL
	Published: August 11, 2020; 10:15:11 AM -0400	V2.0: 6.5 MEDIUM
CVE-2020-14313	An information disclosure vulnerability was found in Red Hat Quay in versions before 3.3.1. This flaw allows an attacker who can create a build trigger in a repository, to disclose the names of robot accounts and the existence of private repositories within any namespace.	V3.1: 4.3 MEDIUM
	Published: August 11, 2020; 10:15:11 AM -0400	V2.0: 4.0 MEDIUM
CVE-2020-14296	Red Hat CloudForms 4.7 and 5 was vulnerable to Server-Side Request Forgery (SSRF) flaw. With the access to add Ansible Tower provider, an attacker could scan and attack systems from the internal network which are not normally accessible.	V3.1: 7.1 HIGH

	Published: August 11, 2020; 10:15:11 AM -0400	V2.0: 5.5 MEDIUM
CVE-2020-10780	Red Hat CloudForms 4.7 and 5 is affected by CSV Injection flaw, a crafted payload stays dormant till a victim export as CSV and opens the file with Excel. Once the victim opens the file, the formula executes, triggering any number of possible events. While this is strictly not an flaw that affects the application directly, attackers could use the loosely validated parameters to trigger several attack possibilities.	V3.1: 7.8 HIGH
	Published: August 11, 2020; 10:15:11 AM -0400	V2.0: 6.8 MEDIUM
CVE-2020-14325	Red Hat CloudForms before 5.11.7.0 was vulnerable to the User Impersonation authorization flaw which allows malicious attacker to create existent and non-existent role-based access control user, with groups and roles. With a selected group of EvmGroup-super_administrator, an attacker can perform any API request as a super administrator.	V3.1: 9.1 CRITICAL
	Published: August 11, 2020; 9:15:12 AM -0400	V2.0: 6.4 MEDIUM
CVE-2020-10783	Red Hat CloudForms 4.7 and 5 is affected by a role-based privilege escalation flaw. An attacker with EVM-Operator group can perform actions restricted only to EVM-Super-administrator group, leads to, exporting or importing administrator files.	V3.1: 8.3 HIGH
	Published: August 11, 2020; 9:15:12 AM -0400	V2.0: 6.5 MEDIUM
CVE-2020-10779	Red Hat CloudForms 4.7 and 5 leads to insecure direct object references (IDOR) and functional level access control bypass due to missing privilege check. Therefore, if an attacker knows the right criteria, it is possible to access some sensitive data within the CloudForms.	V3.1: 6.5 MEDIUM
	Published: August 11, 2020; 9:15:12 AM -0400	V2.0: 4.0 MEDIUM
CVE-2020-10778	In Red Hat CloudForms 4.7 and 5, the read only widgets can be edited by inspecting the forms and dropping the disabled attribute from the fields since there is no server-side validation. This business logic flaw violate the expected behavior.	V3.1: 6.0 MEDIUM
	Published: August 11, 2020; 9:15:12 AM -0400	V2.0: 6.5 MEDIUM
CVE-2020-10777	A cross-site scripting flaw was found in Report Menu feature of Red Hat CloudForms 4.7 and 5. An attacker could use this flaw to execute a stored XSS attack on an application administrator using CloudForms.	V3.1: 5.4 MEDIUM
	Published: August 11, 2020; 9:15:11 AM -0400	V2.0: 3.5 LOW
CVE-2020-4486	IBM QRadar 7.2.0 thorugh 7.2.9 could allow an authenticated user to overwrite or delete arbitrary files due to a flaw after WinCollect installation. IBM X-Force ID: 181861.	V3.1: 8.1 HIGH
	Published: August 11, 2020; 8:15:12 AM -0400	V2.0: 5.5 MEDIUM
CVE-2020-4485	IBM QRadar 7.2.0 through 7.2.9 could allow an authenticated user to disable the Wincollect service which could aid an attacker in bypassing security mechanisms in future attacks. IBM X-Force ID: 181860.	V3.1: 6.5 MEDIUM
	Published: August 11, 2020; 8:15:11 AM -0400	V2.0: 4.0 MEDIUM
CVE-2020-9079	FusionSphere OpenStack 8.0.0 have a protection mechanism failure vulnerability. The product incorrectly uses a protection mechanism. An attacker has to find a way to exploit the vulnerability to conduct directed attacks against the affected product.	V3.1: 8.8 HIGH
	Published: August 10, 2020; 10:15:12 PM -0400	V2.0: 5.8 MEDIUM
CVE-2020-16278	A cross-site scripting (XSS) vulnerability in the Permissions component in SAINT Security Suite 8.0 through 9.8.20 could allow arbitrary script to run in the context of a logged-in user when the user clicks on a specially crafted link.	V3.1: 6.1 MEDIUM
	Published: August 10, 2020; 7:15:12 PM -0400	V2.0: 4.3 MEDIUM
CVE-2020-15820	In JetBrains YouTrack before 2020.2.6881, the markdown parser could disclose hidden file existence.	V3.1: 5.3 MEDIUM
	Published: August 08, 2020; 5:15:11 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-15819	JetBrains YouTrack before 2020.2.10643 was vulnerable to SSRF that allowed scanning internal ports.	V3.1: 5.3 MEDIUM
	Published: August 08, 2020; 5:15:10 PM -0400	V2.0: 5.0 MEDIUM

CVE-2020-15818	In JetBrains YouTrack before 2020.2.8527, the subtasks workflow could disclose issue existence.	V3.1: 5.3 MEDIUM
	Published: August 08, 2020; 5:15:10 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-15817	In JetBrains YouTrack before 2020.1.1331, an external user could execute commands against arbitrary issues.	V3.1: 8.8 HIGH
	Published: August 08, 2020; 5:15:10 PM -0400	V2.0: 6.5 MEDIUM
CVE-2019-19704	In JetBrains Upsource before 2020.1, information disclosure is possible because of an incorrect user matching algorithm.	V3.1: 7.5 HIGH
	Published: August 08, 2020; 5:15:10 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-15065	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to denial-of-service the device via long input values.	V3.1: 6.5 MEDIUM V2.0: 6.1 MEDIUM
	Published: August 07, 2020; 6:15:13 PM -0400	
CVE-2020-15064	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name.	V3.1: 4.3 MEDIUM V2.0: 2.3 LOW
	Published: August 07, 2020; 6:15:13 PM -0400	
CVE-2020-15063	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter.	V3.1: 8.8 HIGH V2.0: 8.3 HIGH
	Published: August 07, 2020; 6:15:13 PM -0400	
CVE-2020-15062	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic.	V3.1: 8.8 HIGH V2.0: 3.3 LOW
	Published: August 07, 2020; 6:15:13 PM -0400	
CVE-2020-15061	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to denial-of-service the device via long input values.	V3.1: 6.5 MEDIUM V2.0: 6.1 MEDIUM
	Published: August 07, 2020; 6:15:13 PM -0400	
CVE-2020-15060	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name.	V3.1: 4.3 MEDIUM V2.0: 2.3 LOW
	Published: August 07, 2020; 6:15:13 PM -0400	
CVE-2020-15059	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter.	V3.1: 8.8 HIGH V2.0: 8.3 HIGH
	Published: August 07, 2020; 6:15:13 PM -0400	
CVE-2020-15058	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic.	V3.1: 8.8 HIGH V2.0: 3.3 LOW
	Published: August 07, 2020; 6:15:13 PM -0400	
CVE-2020-15057	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to denial-of-service the device via long input values.	V3.1: 6.5 MEDIUM V2.0: 6.1 MEDIUM
	Published: August 07, 2020; 6:15:12 PM -0400	
CVE-2020-15056	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name.	V3.1: 4.3 MEDIUM V2.0: 2.3 LOW
	Published: August 07, 2020; 6:15:12 PM -0400	
CVE-2020-15055	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter.	V3.1: 8.8 HIGH V2.0: 8.3 HIGH
	Published: August 07, 2020; 6:15:12 PM -0400	

CVE-2020-15054	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic.	V3.1: 8.8 HIGH
	Published: August 07, 2020; 6:15:12 PM -0400	V2.0: 3.3 LOW
CVE-2019-7005	A vulnerability was discovered in the web interface component of IP Office that may potentially allow a remote, unauthenticated user with network access to gain sensitive information. Affected versions of IP Office include: 9.x, 10.0 through 10.1.0.7 and 11.0 through 11.0.4.2.	V3.1: 7.5 HIGH
	Published: August 07, 2020; 6:15:12 PM -0400	V2.0: 5.0 MEDIUM
CVE-2020-5412	Spring Cloud Netflix, versions 2.2.x prior to 2.2.4, versions 2.1.x prior to 2.1.6, and older unsupported versions allow applications to use the Hystrix Dashboard proxy.stream endpoint to make requests to any server reachable by the server hosting the dashboard. A malicious user, or attacker, can send a request to other servers that should not be exposed publicly.	V3.1: 6.5 MEDIUM
	Published: August 07, 2020; 5:15:10 PM -0400	V2.0: 4.0 MEDIUM
CVE-2020-15480	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics through 7.1, and PerformanceTest through 10. The kernel driver exposes IOCTL functionality that allows low-privilege users to read and write to arbitrary Model Specific Registers (MSRs). This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys.	V3.1: 8.8 HIGH
	Published: August 07, 2020; 5:15:10 PM -0400	V2.0: 7.2 HIGH
CVE-2020-13364	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0.	V3.1: 8.8 HIGH
	Published: August 06, 2020; 1:15:10 PM -0400	V2.0: 9.0 HIGH
CVE-2020-7361	The EasyCorp ZenTao Pro application suffers from an OS command injection vulnerability in its '/pro/repo-create.html' component. After authenticating to the ZenTao dashboard, attackers may construct and send arbitrary OS commands via the POST parameter 'path', and those commands will run in an elevated SYSTEM context on the underlying Windows operating system.	V3.1: 8.8 HIGH
	Published: August 06, 2020; 12:15:13 PM -0400	V2.0: 9.0 HIGH
CVE-2020-7357	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5.	V3.1: 9.9 CRITICAL
	Published: August 06, 2020; 12:15:13 PM -0400	V2.0: 9.0 HIGH
CVE-2020-7356	CAYIN xPost suffers from an unauthenticated SQL Injection vulnerability. Input passed via the GET parameter 'wayfinder_seqid' in wayfinder_meeting_input.jsp is not properly sanitized before being returned to the user or used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code and execute SYSTEM commands.	V3.1: 9.8 CRITICAL
	Published: August 06, 2020; 12:15:13 PM -0400	V2.0: 10.0 HIGH

CVE-2020-7352	The GalaxyClientService component of GOG Galaxy runs with elevated SYSTEM privileges in a Windows environment. Due to the software shipping with embedded, static RSA private key, an attacker with this key material and local user permissions can effectively send any operating system command to the service for execution in this elevated context. The service listens for such commands on a locally-bound network port, localhost:9978. A Metasploit module has been published which exploits this vulnerability. This issue affects the 2.0.x branch of the software (2.0.12 and earlier) as well as the 1.2.x branch (1.2.64 and earlier). A fix was issued for the 2.0.x branch of the affected software. **Published:** August 06, 2020; 12:15:13 PM -0400 **Published:** August 05, 2020; 6:15:12 PM -0400	V3.1: 8.8 HIGH V2.0: 7.2 HIGH
CVE-2020-7298	Unexpected behavior violation in McAfee Total Protection (MTP) prior to 16.0.R26 allows local users to turn off real time scanning via a specially crafted object making a specific function call. **Published:** August 05, 2020; 5:15:12 PM -0400 **Published:** August 05, 2020; 5:15:12 PM -0400	V3.1: 8.4 HIGH V2.0: 3.6 LOW
CVE-2020-15127	In Contour (Ingress controller for Kubernetes) before version 1.7.0, a bad actor can shut down all instances of Envoy, essentially killing the entire ingress data plane. GET requests to /shutdown on port 8090 of the Envoy pod initiate Envoy's shutdown procedure. The shutdown procedure includes flipping the readiness endpoint to false, which removes Envoy from the routing pool. When running Envoy (For example on the host network, pod spec hostNetwork=true), the shutdown manager's endpoint is accessible to anyone on the network that can reach the Kubernetes node that's running Envoy. There is no authentication in place that prevents a rogue actor on the network from shutting down Envoy via the shutdown manager endpoint. Successful exploitation of this issue will lead to bad actors shutting down all instances of Envoy, essentially killing the entire ingress data plane. This is fixed in version 1.7.0. **Published:** August 05, 2020; 5:15:12 PM -0400	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
CVE-2020-13404	The ATOS/Sips (aka Atos-Magento) community module 3.0.0 to 3.0.5 for Magento allows command injection. **Published:** August 05, 2020; 5:15:11 PM -0400	V3.1: 8.8 HIGH V2.0: 9.0 HIGH
CVE-2020-16254	The Chartkick gem through 3.3.2 for Ruby allows Cascading Style Sheets (CSS) Injection (without attribute). **Published:** August 05, 2020; 4:15:14 PM -0400	V3.1: 6.1 MEDIUM V2.0: 4.3 MEDIUM
CVE-2020-15113	In etcd before versions 3.3.23 and 3.4.10, certain directory paths are created (etcd data directory and the directory path when provided to automatically generate self-signed certificates for TLS connections with clients) with restricted access permissions (700) by using the os.MkdirAll. This function does not perform any permission checks when a given directory path exists already. A possible workaround is to ensure the directories have the desired permission (700). **Published:** August 05, 2020; 4:15:14 PM -0400	V3.1: 7.1 HIGH V2.0: 3.6 LOW
CVE-2020-15112	In etcd before versions 3.3.23 and 3.4.10, it is possible to have an entry index greater then the number of entries in the ReadAll method in wal/wal.go. This could cause issues when WAL entries are being read during consensus as an arbitrary etcd consensus participant could go down from a runtime panic when reading the entry. **Published:** August 05, 2020; 4:15:14 PM -0400	V3.1: 6.5 MEDIUM V2.0: 4.0 MEDIUM
CVE-2020-15106	In etcd before versions 3.3.23 and 3.4.10, a large slice causes panic in decodeRecord method. The size of a record is stored in the length field of a WAL file and no additional validation is done on this data. Therefore, it is possible to forge an extremely large frame size that can unintentionally panic at the expense of any RAFT participant trying to decode the WAL. **Published:** August 05, 2020; 3:15:10 PM -0400	V3.1: 6.5 MEDIUM V2.0: 4.0 MEDIUM

CVE-2020-16192	LimeSurvey 4.3.2 allows reflected XSS because application/controllers/LSBaseController.php lacks code to validate parameters. **Published:** August 05, 2020; 12:15:12 PM -0400	V3.1: 6.1 MEDIUM V2.0: 4.3 MEDIUM
CVE-2020-17364	USVN (aka User-friendly SVN) before 1.0.9 allows XSS via SVN logs. **Published:** August 05, 2020; 11:15:13 AM -0400	V3.1: 6.1 MEDIUM V2.0: 4.3 MEDIUM
CVE-2020-8607	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **Published:** August 05, 2020; 10:15:13 AM -0400	V3.1: 6.7 MEDIUM V2.0: 7.2 HIGH
CVE-2020-5609	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors. **Published:** August 05, 2020; 10:15:13 AM -0400	V3.1: 9.8 CRITICAL V2.0: 7.5 HIGH
CVE-2020-5608	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **Published:** August 05, 2020; 10:15:13 AM -0400	V3.1: 9.8 CRITICAL V2.0: 7.5 HIGH