BGD e-GOV CIRT

BGD e-GOV CIRT project
Common Vulnerabilities and Exposures (CVE) Report

Issue Date: 01-July-2020 **Issue Number:07**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Microsoft				
Windows SMBv3 Client/Server Information Disclosure Vulnerability	09-June-2020	**8.6** **HIGH**	**CVE-2020-1206** An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1206
Remote Code Execution Vulnerability	09-June-2020	**8.4** **HIGH**	**CVE-2020-1248** A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	-
Windows SMBv3 Client/Server Denial of Service Vulnerability	09-June-2020	**7.5** **HIGH**	**CVE-2020-1284** A denial of service vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Denial of Service Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1284
Windows SMB Authenticated Remote Code	09-June-2020	**7.5** **HIGH**	**CVE-2020-1301** A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1)	https://portal.msrc.microsoft.com/en-US/security-

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Execution Vulnerability			server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'.	guidance/advisory/CVE-2020-1301
Windows Runtime Information Disclosure Vulnerability	09-June-2020	**7.0** **HIGH**	**CVE-2020-1217** An information disclosure vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1217
Media Foundation Information Disclosure Vulnerability	09-June-2020	**6.5** **Medium**	**CVE-2020-1232** An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1232
Windows Error Reporting Information Disclosure Vulnerability	09-June-2020	**5.5** **Medium**	**CVE-2020-1261 & CVE-2020-1263** An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1263.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1261 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1263
Windows Service Information Disclosure Vulnerability	09-June-2020	**5.5** **Medium**	**CVE-2020-1268** An information disclosure vulnerability exists when a Windows service improperly handles objects in memory, aka 'Windows Service Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1268
Win32k Information Disclosure Vulnerability	09-June-2020	**5.5** **Medium**	**CVE-2020-1290** An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1290
Windows GDI Information Disclosure Vulnerability	12-May-2020	**5.5** **Medium**	**CVE-2020-0963** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0963

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179.	
Windows Kernel Information Disclosure Vulnerability	12-May-2020	**5.5** **Medium**	**CVE-2020-1072** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1072
Windows Subsystem for Linux Information Disclosure Vulnerability	12-May-2020	**5.5** **Medium**	**CVE-2020-1075** An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka 'Windows Subsystem for Linux Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1075
Windows CSRSS Information Disclosure Vulnerability	12-May-2020	**5.5** **Medium**	**CVE-2020-1116** An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1116
Windows GDI Information Disclosure Vulnerability	12-May-2020	**5.5** **Medium**	**CVE-2020-1141** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1145, CVE-2020-1179.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1141
Windows GDI Information Disclosure Vulnerability	12-May-2020	**5.5** **Medium**	**CVE-2020-1145** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1145

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1179.	
Microsoft Power BI Report Server Spoofing Vulnerability	12-May-2020	**5.5 Medium**	**CVE-2020-1173** A spoofing vulnerability exists in Microsoft Power BI Report Server in the way it validates the content-type of uploaded attachments, aka 'Microsoft Power BI Report Server Spoofing Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1173
Application: Cisco				
SaltStack FrameWork Vulnerabilities Affecting Cisco Products	28-May-2020	**10 Critical**	**CVE-2020-11651** **CVE-2020-11652** Cisco Modeling Labs Corporate Edition (CML), Cisco TelePresence IX5000 Series, and Cisco Virtual Internet Routing Lab Personal Edition (VIRL-PE) incorporate a version of SaltStack that is running the salt-master service that is affected by these vulnerabilities.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-salt-2vx545AG
Telnet Vulnerability Affecting Cisco Products	24-June-2020	**9.8 Critical**	**CVE-2020-10188** Cisco investigated its product line to determine which products may be affected by this vulnerability. The Vulnerable Products section includes Cisco bug IDs for each affected product. The bugs are accessible through the Cisco Bug Search Tool and contain additional platform-specific information, including workarounds (if available) and fixed software releases.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-telnetd-EFJrEzPx
Cisco IOS Software for Cisco Industrial Routers Arbitrary Code Execution Vulnerabilities	03-June-2020	**9.8 Critical**	**CVE-2020-3198** **CVE-2020-3258** Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-rce-xYRSeMNH

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload.	
Cisco Unified Contact Center Express Remote Code Execution Vulnerability	20-May-2020	**9.8** **Critical**	**CVE-2020-3280** A vulnerability in the Java Remote Management Interface of Cisco Unified Contact Center Express (Unified CCX) could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-rce-GMSC6RKN
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Path Traversal Vulnerability	06-May-2020	**9.1** **Critical**	**CVE-2020-3187** A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and obtain read and delete access to sensitive files on a targeted system.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-path-JE3azWw43
Cisco IOS, IOS XE, IOS XR, and NX-OS Software One Platform Kit Remote Code Execution Vulnerability	03-June-2020	**8.8** **HIGH**	**CVE-2020-3217** A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-nxos-onepk-rce-6Hhyt4dC
Cisco IOS XE Software Web UI Command Injection Vulnerability	03-June-2020	**8.8** **HIGH**	**CVE-2020-3224** A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with read-only privileges to inject IOS commands to an affected device. The injected commands should require a higher privilege level in order to be executed.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-cmdinj-zM283Zdw

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Cisco IOS XE Software Web UI Privilege Escalation Vulnerability	03-June-2020	**8.8** **HIGH**	**CVE-2020-3229** A vulnerability in Role Based Access Control (RBAC) functionality of Cisco IOS XE Web Management Software could allow a Read-Only authenticated, remote attacker to execute commands or configuration changes as an Admin user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-PZgQxjfG
Cisco IOS XE Software Web UI Command Injection Vulnerability	03-June-2020	**8.8** **HIGH**	**CVE-2020-3219** A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to inject and execute arbitrary commands with administrative privileges on the underlying operating system of an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-web-cmdinj2-fOnjk2LD
Cisco IOS Software for Cisco Industrial Routers Virtual Device Server Inter-VM Channel Command Injection Vulnerability	03-June-2020	**8.8** **HIGH**	**CVE-2020-3205** A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-udp-vds-inj-f2D5Jzrt
Cisco IOS Software for Cisco Industrial Routers Virtual Device Server Static Credentials Vulnerability	03-June-2020	**8.8** **HIGH**	**CVE-2020-3234** A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-vds-cred-uPMp9zbY
Cisco NX-OS Software Unexpected IP in IP	01-June-2020	**8.6** **HIGH**	**CVE-2020-10136** A vulnerability in the network stack of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Packet Processing Vulnerability			bypass certain security boundaries or cause a denial of service (DoS) condition on an affected device.	nxos-ipip-dos-kCT9X4
Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability	06-May-2020	**8.6** **HIGH**	**CVE-2020-3283** A vulnerability in the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) handler of Cisco Firepower Threat Defense (FTD) Software when running on the Cisco Firepower 1000 Series platform could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-dos-4v5nmWtZ
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software OSPF Packets Processing Memory Leak Vulnerability	06-May-2020	**8.6** **HIGH**	**CVE-2020-3195** A vulnerability in the Open Shortest Path First (OSPF) implementation in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ospf-memleak-DHpsgfnv
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Malformed OSPF Packets Processing Denial of Service Vulnerability	06-May-2020	**8.6** **HIGH**	**CVE-2020-3298** A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the reload of an affected device, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ospf-dos-RhMQY8qx
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Media Gateway Control Protocol Denial of Service Vulnerabilities	06-May-2020	**8.6** **HIGH**	**CVE-2020-3254** Multiple vulnerabilities in the Media Gateway Control Protocol (MGCP) inspection feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgcp-SUqB8VKH

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software IPv6 DNS Denial of Service Vulnerability	06-May-2020	**8.6** **HIGH**	**CVE-2020-3191** A vulnerability in DNS over IPv6 packet processing for Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to unexpectedly reload, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ipv6-67pA658k
Cisco Firepower Threat Defense Software VPN System Logging Denial of Service Vulnerability	06-May-2020	**8.6** **HIGH**	**CVE-2020-3189** A vulnerability in the VPN System Logging functionality for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak that can deplete system memory over time, which can cause unexpected system behaviors or device crashes.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-Rdpe34sd8
Cisco Firepower Threat Defense Software Generic Routing Encapsulation Tunnel IPv6 Denial of Service Vulnerability	06-May-2020	**8.6** **HIGH**	**CVE-2020-3179** A vulnerability in the generic routing encapsulation (GRE) tunnel decapsulation feature of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-2-sS2h7aWe
Cisco IOS and IOS XE Software Common Industrial Protocol Denial of Service Vulnerabilities	03-June-2020	**8.6** **HIGH**	**CVE-2020-3225** Multiple vulnerabilities in the implementation of the Common Industrial Protocol (CIP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cipdos-hkfTZXEx
Cisco IOx Application Framework Arbitrary File Creation Vulnerability	03-June-2020	**8.1** **HIGH**	**CVE-2020-3238** A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-caf-3dXM8exv

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			attacker to write or modify arbitrary files in the virtual instance that is running on the affected device.	
Cisco IOx Application Environment for IOS Software for Cisco Industrial Routers Vulnerabilities	03-June-2020	**8.1** **HIGH**	**CVE-2020-3199** **CVE-2020-3257** Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-gos-vuln-s9qS8kYL
Cisco Webex Meetings and Cisco Webex Meetings Server Token Handling Unauthorized Access Vulnerability	17-June-2020	**8.1** **HIGH**	**CVE-2020-3361** A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to gain unauthorized access to a vulnerable Webex site.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-token-zPvEjKN
Cisco Webex Meetings Desktop App URL Filtering Arbitrary Program Execution Vulnerability	17-June-2020	**7.5** **HIGH**	**CVE-2020-3263** A vulnerability in Cisco Webex Meetings Desktop App could allow an unauthenticated, remote attacker to execute programs on an affected end-user system.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-url-fcmpdfVY
Cisco TelePresence Collaboration Endpoint and RoomOS Software Command Injection Vulnerability	17-June-2020	**7.2** **HIGH**	**CVE-2020-3336** A vulnerability in the software upgrade process of Cisco TelePresence Collaboration Endpoint Software and Cisco RoomOS Software could allow an authenticated, remote attacker to modify the filesystem to cause a denial of service (DoS) or gain privileged access to the root filesystem.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tp-cmd-inj-7ZpWhvZb
Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution Vulnerabilities	17-June-2020	**7.2** **HIGH**	**CVE-2020-3286** **CVE-2020-3287** **CVE-2020-3288** **CVE-2020-3289** **CVE-2020-3290** **CVE-2020-3291**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-stack-vUxHmnNz

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			CVE-2020-3292 **CVE-2020-3293** **CVE-2020-3294** **CVE-2020-3295** **CVE-2020-3296** Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device.	
Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers Management Interface Vulnerabilities	17-June-2020	**7.2** **HIGH**	**CVE-2020-3268** **CVE-2020-3269** Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-injection-tWC7krKQ
Cisco Small Business RV Series Routers Command Injection Vulnerabilities	17-June-2020	**7.2** **HIGH**	**CVE-2020-3274** **CVE-2020-3275** **CVE-2020-3276** **CVE-2020-3277** **CVE-2020-3278** **CVE-2020-3279** Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-Rj5JRfF8
Cisco IOS XE Software Web UI Command Injection Vulnerability	03-June-2020	**7.2** **HIGH**	**CVE-2020-3211** A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-web-cmdinj4-S2TmH7GA
Cisco IOS XE Software Web UI	03-June-2020	**7.2** **HIGH**	**CVE-2020-3212**	https://tools.cisco.com/security/center/

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Command Injection Vulnerability			A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device.	content/CiscoSecurityAdvisory/cisco-sa-web-cmdinj3-44st5CcA
Cisco Enterprise NFV Infrastructure Software Path Traversal Vulnerability	17-June-2020	**6.7 Medium**	**CVE-2020-3236** A vulnerability in the CLI of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to gain root shell access to the underlying operating system and overwrite or read arbitrary files. The attacker would need valid administrative credentials.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-ptrav-SHMzzwVR
Cisco UCS Director Path Traversal Vulnerability	17-June-2020	**6.5 Medium**	**CVE-2020-3241** A vulnerability in the orchestration tasks of Cisco UCS Director could allow an authenticated, remote attacker to perform a path traversal attack on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsd-task-path-trav-d67ZuAk7
Application: Apache				
Apache Syncope vulnerability	04-April-2020	**9.8 Critical**	**CVE-2020-1959** A Server-Side Template Injection was identified in Apache Syncope prior to 2.1.6 enabling attackers to inject arbitrary Java EL expressions, leading to an unauthenticated Remote Code Execution (RCE) vulnerability. Apache Syncope uses Java Bean Validation (JSR 380) custom constraint validators. When building custom constraint violation error messages, they support different types of interpolation, including Java EL expressions. Therefore, if an attacker can inject arbitrary data in the error message template being passed, they will be able to run arbitrary Java code.	Patch: Fixed in release 2.1.6 http://syncope.apache.org/security
Apache Syncope vulnerability	04-April-2020	**9.8 Critical**	**CVE-2020-1961** Vulnerability to Server-Side Template Injection on Mail templates for Apache Syncope 2.0.X releases prior to 2.0.15, 2.1.X releases prior to 2.1.6, enabling attackers to inject arbitrary JEXL	Fixed in release 2.0.15, release 2.1.6. http://syncope.apache.org/security

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			expressions, leading to Remote Code Execution (RCE) was discovered.	
Apache log4net vulnerability	11-May-2020	**9.8** **Critical**	**CVE-2018-1285** Apache log4net before 2.0.8 does not disable XML external entities when parsing log4net configuration files. This could allow for XXE-based attacks in applications that accept arbitrary configuration files from users.	https://lists.apache.org/thread.html/reab1c277c95310bad1038255e0757857b2fbe291411b4fa84552028a%40%3Cdev.logging.apache.org%3E https://issues.apache.org/jira/browse/LOG4NET-575
Apache Unomi vulnerability	05-June-2020	**9.8** **Critical**	**CVE-2020-11975** Apache Unomi allows conditions to use OGNL scripting which offers the possibility to call static Java classes from the JDK that could execute code with the permission level of the running Java process.	http://unomi.apache.org/security/cve-2020-11975.txt
Apache Kylin vulnerability	22-May-2020	**8.8** **HIGH**	**CVE-2020-1956** Apache Kylin 2.3.0, and releases up to 2.6.5 and 3.0.1 has some restful apis which will concatenate os command with the user input string, a user is likely to be able to execute any os command without any protection or validation.	https://lists.apache.org/thread.html/r1332ef34cf8e2c0589cf44ad269fb1fb4c06addec6297f0320f5111d%40%3Cuser.kylin.apache.org%3E
Apache Tomcat Denial of Service vulnerability	21-June-2020	**7.5** **HIGH**	**CVE-2019-10072** The fix for CVE-2019-0199 was incomplete and did not address HTTP/2 connection window exhaustion on write in Apache Tomcat versions 9.0.0.M1 to 9.0.19 and 8.5.0 to 8.5.40 . By not sending WINDOW_UPDATE messages for the connection window (stream 0) clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS.	apache-tomcat-upgrade-8_5_41/apache-tomcat-upgrade-9_0_20 https://lists.apache.org/thread.html/df1a2c1b87c8a6c500ecdbbaf134c7f1491c8d79d98b48c6b9f0fa6a@%3Cannounce.tomcat.apache.org%3E

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Apache Tomcat HTTP/2 Denial of Service	26-June-2020		**CVE-2020-11996** A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.	- Upgrade to Apache Tomcat 10.0.0-M6 or later - Upgrade to Apache Tomcat 9.0.36 or later - Upgrade to Apache Tomcat 8.5.56 or later http://mail-archives.us.apache.org/mod_mbox/www-announce/202006.mbox/<fd56bc1d-1219-605b-99c7-946bf7bd8ad4%40apache.org> https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E https://lists.apache.org/thread.html/rea65d6ef2e45dd1c45faae8392204273286 6c7b88fa109b76c83db52@%3Cnotifications.ofbiz.apache.org%3E http://tomcat.apache.org/security-10.html http://tomcat.apache.org/security-9.html http://tomcat.apache.org/security-8.htm
Application: Github-enterprise server				
github -- enterprise server vulnerability	03-June-2020	**9.8 Critical**	**CVE-2020-10516** An improper access control vulnerability was identified in the GitHub Enterprise Server API that	https://enterprise.github.com/releases/2.18.20/notes

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			allowed an organization member to escalate permissions and gain access to unauthorized repositories within an organization. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.21 and was fixed in 2.20.9, 2.19.15, and 2.18.20.	https://enterprise.github.com/releases/2.19.15/notes https://enterprise.github.com/releases/2.20.9/notes
Application: FreeBSD				
Insufficient cryptodev MAC key length check	12-May-2020	**9.8 Critical**	**CVE-2019-15880** In FreeBSD 12.1-STABLE before r356911, and 12.1-RELEASE before p5, insufficient checking in the cryptodev module allocated the size of a kernel buffer based on a user-supplied length allowing an unprivileged process to trigger a kernel panic.	https://security.freebsd.org/advisories/FreeBSD-SA-20:16.cryptodev.asc https://security.netapp.com/advisory/ntap-20200518-0008/
Insufficient packet length validation in libalias	12-May-2020	**9.8 Critical**	**CVE-2020-7454** In FreeBSD 12.1-STABLE before r360971, 12.1-RELEASE before p5, 11.4-STABLE before r360971, 11.4-BETA1 before p1 and 11.3-RELEASE before p9, libalias does not properly validate packet length resulting in modules causing an out of bounds read/write condition if no checking was built into the module.	https://security.freebsd.org/advisories/FreeBSD-SA-20:12.libalias.asc https://security.netapp.com/advisory/ntap-20200518-0005/
Application: IBM				
IBM Data Risk Manager Vulnerability	28-May-2020	**9.8 Critical**	**CVE-2020-4427** IBM Data Risk Manager 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, and 2.0.6 could allow a remote attacker to bypass security restrictions when configured with SAML authentication. By sending a specially crafted HTTP request, an attacker could exploit this vulnerability to bypass the authentication process and gain full administrative access to the system. IBM X-Force ID: 180532.	https://www.ibm.com/support/pages/node/6206875 https://exchange.xforce.ibmcloud.com/vulnerabilities/180532
IBM Data Risk Manage Vulnerability	28-May-2020	**9.8 Critical**	**CVE-2020-4429** IBM Data Risk Manager 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, and 2.0.6 contains a default password for an IDRM administrative account. A remote attacker could exploit this vulnerability	https://www.ibm.com/support/pages/node/6206875 https://exchange.xforce.ibmcloud.com/

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			to login and execute arbitrary code on the system with root privileges. IBM X-Force ID: 180534.	vulnerabilities/180534
IBM Data Risk Manage Vulnerability	28-May-2020	**9.1 Critical**	**CVE-2020-4428** IBM Data Risk Manager 2.0.1, 2.0.2, 2.0.3, and 2.0.4 could allow a remote authenticated attacker to execute arbitrary commands on the system. IBM X-Force ID: 180533.	https://www.ibm.com/support/pages/node/6206875 https://exchange.xforce.ibmcloud.com/vulnerabilities/180533
Application: Google Chrome Launcher				
Google Chrome launcher Vulnerability	07-May-2020	**9.8 Critical**	**CVE-2020-7645** All versions of chrome-launcher allow execution of arbitrary commands, by controlling the $HOME environment variable in Linux operating systems.	Upgrade chrome-launcher to version 0.13.2 or higher.
Application: Samsung				
Samsung's Android OS versions O(8.x), P(9.0) and Q(10.0) Vulnerability	06-May-2020	**9.8 Critical**	**CVE-2020-8899** There is a buffer overwrite vulnerability in the Quram qmg library of Samsung's Android OS versions O(8.x), P(9.0) and Q(10.0). An unauthenticated, unauthorized attacker sending a specially crafted MMS to a vulnerable phone can trigger a heap-based buffer overflow in the Quram image codec leading to an arbitrary remote code execution (RCE) without any user interaction. The Samsung ID is SVE-2020-16747.	https://security.samsungmobile.com/securityUpdate.smsb
Samsung mobile devices with O(8.x) and P(9.0) (Exynos 7570 chipsets) software vulnerability	04-June-2020	**9.8 Critical**	**CVE-2020-13831** An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 7570 chipsets) software. The Trustonic Kinibi component allows arbitrary memory mapping. The Samsung ID is SVE-2019-16665 (June 2020).	https://security.samsungmobile.com/securityUpdate.smsb
Application: Linux Kernel				
Linux kernel vulnerability	05-May-2020	**7.1 HIGH**	**CVE-2020-12654** An issue was found in Linux kernel before 5.5.4.	https://cdn.kernel.org/pub/linux/kernel

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			mwifiex_ret_wmm_get_status() in drivers/net/wireless/marvell/mwifiex/wmm.c allows a remote AP to trigger a heap-based buffer overflow because of an incorrect memcpy, aka CID-3a9b153c5591.	/v5.x/ChangeLog-5.5.4 https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=3a9b153c5591548612c3955c9600a98150c81875 https://github.com/torvalds/linux/commit/3a9b153c5591548612c3955c9600a98150c81875
Linux kernel vulnerability	05-May-2020	**6.7 MEDIUM**	**CVE-2020-12659** An issue was discovered in the Linux kernel before 5.6.7. xdp_umem_reg in net/xdp/xdp_umem.c has an out-of-bounds write (by a user with the CAP_NET_ADMIN capability) because of a lack of headroom validation.	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.6.7 https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=99e3a236dd43d06c65af0a2ef9cb44306aef6e02 https://github.com/torvalds/linux/commit/99e3a236dd43d06c65af0a2ef9cb44306aef6e02
Application: Palo Alto Networks - PAN-OS				
PAN-OS Panorama External control of file vulnerability leads to privilege escalation	13-May-2020	**9.8 Critical**	**CVE-2020-2001** An external control of path and data vulnerability in the Palo Alto Networks PAN-OS Panorama XSLT processing logic that allows an unauthenticated user with network access to PAN-OS management interface to write attacker supplied file on the system and elevate privileges. This issue affects: All PAN-OS 7.1 Panorama and 8.0 Panorama versions; PAN-OS 8.1 versions earlier than 8.1.12 on Panorama; PAN-OS 9.0 versions earlier than 9.0.6 on Panorama.	This issue is fixed in PAN-OS 8.1.12, PAN-OS 9.0.6, and all later PAN-OS versions. https://security.paloaltonetworks.com/CVE-2020-2001

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
PAN-OS Panorama authentication bypass vulnerability	13-May-2020	**9.0 Critical**	**CVE-2020-2018:** An authentication bypass vulnerability in the Panorama context switching feature allows an attacker with network access to a Panorama's management interface to gain privileged access to managed firewalls. An attacker requires some knowledge of managed firewalls to exploit this issue. This issue does not affect Panorama configured with custom certificates authentication for communication between Panorama and managed devices. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.12; PAN-OS 9.0 versions earlier than 9.0.6; All versions of PAN-OS 8.0.	This issue is fixed in PAN-OS 7.1.26, PAN-OS 8.1.12, PAN-OS 9.0.6, and all later PAN-OS versions. https://security.paloaltonetworks.com/CVE-2020-2018
PAN-OS OS injection vulnerability in PAN-OS management server	13-May-2020	**8.8 HIGH**	**CVE-2020-2014** An OS Command Injection vulnerability in PAN-OS management server allows authenticated users to inject and execute arbitrary shell commands with root privileges. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7.	This issue is fixed in PAN-OS 8.1.14, PAN-OS 9.0.7, PAN-OS 9.1.0 and all later PAN-OS versions. https://security.paloaltonetworks.com/CVE-2020-2014
PAN-OS Buffer overflow in the management server	13-May-2020	**8.8 HIGH**	**CVE-2020-2015** A buffer overflow vulnerability in the PAN-OS management server allows authenticated users to crash system processes or potentially execute arbitrary code with root privileges. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.7; PAN-OS 9.1 versions earlier than 9.1.1; All versions of PAN-OS 8.0.	This issue is fixed in PAN-OS 7.1.26, PAN-OS 8.1.13, PAN-OS 9.0.7, PAN-OS 9.1.1, and all later PAN-OS versions. https://security.paloaltonetworks.com/CVE-2020-2015
PAN-OS Panorama registration denial of service	20-May-2020	**7.5 HIGH**	**CVE-2020-2011** An improper input validation vulnerability in the configuration daemon of Palo Alto Networks PAN-OS Panorama allows for a remote	This issue is fixed in PAN-OS 8.1.14, PAN-OS 9.0.7, PAN-OS 9.1.0 and all later PAN-OS versions.

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			unauthenticated user to send a specifically crafted registration request to the device that causes the configuration service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS Panorama services by restarting the device and putting it into maintenance mode. This issue affects: All versions of PAN-OS 7.1, PAN-OS 8.0; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7; PAN-OS 9.1 versions earlier than 9.1.0.	https://security.paloaltonetworks.com/CVE-2020-2011
PAN-OS Authenticated user command injection vulnerability	13-May-2020	**7.2** **HIGH**	**CVE-2020-2010** An OS command injection vulnerability in PAN-OS management interface allows an authenticated administrator to execute arbitrary OS commands with root privileges. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7.	This issue is fixed in PAN-OS 8.1.14, PAN-OS 9.0.7, PAN-OS 9.1.0, and all later PAN-OS versions. https://security.paloaltonetworks.com/CVE-2020-2010
PAN-OS Panorama SD WAN arbitrary file creation	13-May-2020	**7.2** **HIGH**	**CVE-2020-2009** An external control of filename vulnerability in the SD WAN component of Palo Alto Networks PAN-OS Panorama allows an authenticated administrator to send a request that results in the creation and write of an arbitrary file on all firewalls managed by the Panorama. In some cases this results in arbitrary code execution with root permissions. This issue affects: All versions of PAN-OS 7.1; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7.	https://security.paloaltonetworks.com/CVE-2020-2009
PAN-OS Buffer overflow in authd authentication response	10-June-2020	**7.2** **HIGH**	**CVE-2020-2027** A buffer overflow vulnerability in the authd component of the PAN-OS management server allows authenticated administrators to disrupt system processes and potentially execute arbitrary code with	This issue is fixed in PAN-OS 8.1.13, PAN-OS 9.0.7, PAN-OS 9.1.0, and all later PAN-OS versions.

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			root privileges. This issue affects: All versions of PAN-OS 7.1 and PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13; PAN-OS 9.0 versions earlier than PAN-OS 9.0.7.	https://security.paloaltonetworks.com/CVE-2020-2027
PAN-OS OS command injection vulnerability in management interface certificate generator	10-June-2020	**7.2** **HIGH**	**CVE-2020-2029** An OS Command Injection vulnerability in the PAN-OS web management interface allows authenticated administrators to execute arbitrary OS commands with root privileges by sending a malicious request to generate new certificates for use in the PAN-OS configuration. This issue affects: All versions of PAN-OS 8.0; PAN-OS 7.1 versions earlier than PAN-OS 7.1.26; PAN-OS 8.1 versions earlier than PAN-OS 8.1.13.	This issue is fixed in PAN-OS 7.1.26, PAN-OS 8.1.13, and all later PAN-OS versions. https://security.paloaltonetworks.com/CVE-2020-2029
GlobalProtect App File race condition vulnerability leads to local privilege escalation during upgrade	10-June-2020	**7.0** **HIGH**	**CVE-2020-2032** A race condition vulnerability Palo Alto Networks GlobalProtect app on Windows allows a local limited Windows user to execute programs with SYSTEM privileges. This issue can be exploited only while performing a GlobalProtect app upgrade. This issue affects: GlobalProtect app 5.0 versions earlier than GlobalProtect app 5.0.10 on Windows; GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.4 on Windows.	This issue is fixed in GlobalProtect app 5.0.10, GlobalProtect app 5.1.4, and all later GlobalProtect app versions. https://security.paloaltonetworks.com/CVE-2020-2032
Application: Wordpress				
Elementor Pro < 2.9.4 - Authenticated Arbitrary File Upload	16-May-2020	**9.9** **Critical**	**CVE-2020-13126** An issue was discovered in the Elementor Pro plugin before 2.9.4 for WordPress, as exploited in the wild in May 2020 in conjunction with CVE-2020-13125. An attacker with the Subscriber role can upload arbitrary executable files to achieve remote code execution. NOTE: the free Elementor plugin is unaffected.	Fixed in version 2.9.4 https://wpvulndb.com/vulnerabilities/10214 CVE-2020-13693: WordPress BBPress 2.5 Privilege Escalation

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
WordPress BBPress 2.5 Privilege Escalation	28-May-2020	**9.8 Critical**	**CVE-2020-13693** An unauthenticated privilege-escalation issue exists in the bbPress plugin before 2.6.5 for WordPress when New User Registration is enabled.	bbPress 2.6.5. https://bbpress.org/blog/2020/05/bbpress-2-6-5-is-out/ https://codex.bbpress.org/releases/ https://wordpress.org/plugins/bbpress/#developers
WordPress Drag And Drop Multi File Uploader Remote Code Execution	08-June-2020	**9.8 Critical**	**CVE-2020-12800** The drag-and-drop-multiple-file-upload-contact-form-7 plugin before 1.3.3.3 for WordPress allows Unrestricted File Upload and remote code execution by setting supported_type to php% and uploading a .php% file.	https://wordpress.org/plugins/drag-and-drop-multiple-file-upload-contact-form-7/#developers
WordPress chopSlider 3.3.4 SQL Injection	08-May-2020	**9.8 Critical**	**CVE-2020-11530** A blind SQL injection vulnerability is present in Chop Slider 3, a WordPress plugin. The vulnerability is introduced in the id GET parameter supplied to get_script/index.php, and allows an attacker to execute arbitrary SQL queries in the context of the WP database user.	http://seclists.org/fulldisclosure/2020/May/26 https://github.com/idangerous/Plugins/tree/master/Chop%20Slider%203
Simple File List improper limitation of a pathname to a restricted drectory	13-May-2020	**9.8 Critical**	**CVE-2020-12832** WordPress Plugin Simple File List before 4.2.8 is prone to a vulnerability that lets attackers delete arbitrary files because the application fails to properly verify user-supplied input.	https://plugins.trac.wordpress.org/changeset/2302759 https://wordpress.org/plugins/simple-file-list/#developers
Elementor Pro < 2.9.4 - Authenticated Arbitrary File Upload	16-May-2020	**7.2 HIGH**	**CVE-2020-13125** An issue was discovered in the "Ultimate Addons for Elementor" plugin before 1.24.2 for WordPress, as exploited in the wild in May 2020 in conjunction with CVE-2020-13126. Unauthenticated attackers can create users with the Subscriber role even if registration is disabled.	Fixed in version 2.9.4 https://wpvulndb.com/vulnerabilities/10214 https://www.wordfence.com/blog/2020/05/combined-attack-on-elementor-pro-and-ultimate-addons-

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
				for-elementor-puts-1-million-sites-at-risk/
Application: Aruba Product : ClearPass				
ClearPass Policy Manager Multiple Vulnerabilities	03-June-2020	**9.9** **Critical**	**CVE-2020-7115, CVE-2020-7116, CVE-2020-7117** ClearPass Policy Manager Multiple Vulnerabilities Aruba has released updates to ClearPass Policy Manager that address multiple security vulnerabilities. Affected Products ================= ClearPass 6.9.x prior to 6.9.1 ClearPass 6.8.x prior to 6.8.5-HF ClearPass 6.7.x prior to 6.7.13-HF	1. Upgrade ClearPass Policy Manager 6.9.x to version 6.9.1 2. Upgrade ClearPass Policy Manager 6.8.x to version 6.8.5-HF or 6.8.6 3. Upgrade ClearPass Policy Manager 6.7.x to version 6.7.13-HF https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-005.txt
Application: D-Link				
Unauthenticated Command Bypass to Elevated Privileges	11-May-2020	**9.8** **Critical**	**CVE-2019-18666** An issue was discovered on D-Link DAP-1360 revision F devices. Remote attackers can start a telnet service without authorization via an undocumented HTTP request. Although this is the primary vulnerability, the impact depends on the firmware version. Versions 609EU through 613EUbeta were tested. Versions through 6.12b01 have weak root credentials, allowing an attacker to gain remote root access. After 6.12b01, the root credentials were changed but the telnet service can still be started without authorization.	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10171
D-Link DIR-865L Command Injection vulnerability	03-June-2020	**9.8** **Critical**	**CVE-2020-13782** D-Link DIR-865L Ax 1.20B01 Beta devices allow Command Injection.	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10174

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
		🟥		
Application: Huawei				
Out of Bounds Read Vulnerability in Several Smartphones	13-May-2020	**7.1 HIGH**	**CVE-2020-1808** Huawei smartphones Honor View 20;Honor 20;Honor 20 PRO;Honor Magic2 with Versions earlier than 10.0.0.179(C636E3R4P3),Versions earlier than 10.0.0.180(C185E3R3P3),Versions earlier than 10.0.0.180(C432E10R3P4),Versions earlier than 10.0.0.188(C00E62R2P11);Versions earlier than 10.0.0.187(C00E60R4P11);Versions earlier than 10.0.0.187(C00E60R4P11);Versions earlier than 10.0.0.176(C00E60R2P11) have an out of bound read vulnerability. The software reads data past the end of the intended buffer. The attacker tricks the user into installing a crafted application, successful exploit may cause information disclosure or service abnormal.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200513-02-smartphone-en
Improper Authorization Vulnerability in Some Huawei Smartphones	10-June-2020	**6.8 MEDIUM**	**CVE-2020-1813** HUAWEI P30 smart phone with versions earlier than 10.1.0.135(C00E135R2P11) have an improper authentication vulnerability. Due to improper authentication of specific interface, in specific scenario attackers could access specific interface without authentication. Successful exploit could allow the attacker to perform unauthorized operations.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200610-04-smartphone-en
Denial of Service Vulnerability in Huawei FusionAccess Product	10-June-2020	**6.5 MEDIUM**	**CVE-2020-1825** FusionAccess with versions earlier than 6.5.1.SPC002 have a Denial of Service (DoS) vulnerability. Due to insufficient verification on specific input, attackers can exploit this vulnerability by sending constructed messages to the affected device through another device on the	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200610-01-fusionacces-en

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			same network. Successful exploit could cause affected devices to be abnormal.	
Insufficient Input Verification of Some Huawei products	15-June-2020	**6.5 MEDIUM**	**CVE-2020-9075** Huawei products Secospace USG6300;USG6300E with versions of V500R001C30,V500R001C50,V500R001C60,V500R001C80,V500R005C00,V500R005C10;V600R006C00 have a vulnerability of insufficient input verification. An attacker with limited privilege can exploit this vulnerability to access a specific directory. Successful exploitation of this vulnerability may lead to information leakage.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200610-02-validation-en
Application: MISP				
MISP MISP-maltego 1.4.4 vulnerability	15-May-2020	**9.8 Critical**	**CVE-2020-12889** MISP MISP-maltego 1.4.4 incorrectly shares a MISP connection across users in a remote-transform use case.	https://github.com/MISP/MISP-maltego/commit/3ccde66dab4096ab5663e69f352992cc73e1160b
Application: Mikrotik				
Mikrotik-Router-Monitoring-System	16-May-2020	**9.8 Critical**	**CVE-2020-13118** An issue was discovered in Mikrotik-Router-Monitoring-System through 2018-10-22. SQL Injection exists in check_community.php via the parameter community.	-
Application: WSO2				
WSO2 API Manager	20-May-2020	**9.8 Critical**	**CVE-2020-13226** WSO2 API Manager 3.0.0 does not properly restrict outbound network access from a Publisher node, opening up the possibility of SSRF to this node's entire intranet.	https://docs.wso2.com/display/Security/Security+Advisories https://docs.wso2.com/display/Security/WSO2+Security+Vulnerability+Management+Process https://github.com/wso2/docs-apim/issues/816

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
				https://github.com/wso2/product-apim/issues/7677
Application: Zoom				
Zoom Client path traversal vulnerability	08-June-2020	**9.8 Critical**	**CVE-2020-6109** An exploitable path traversal vulnerability exists in the Zoom client, version 4.6.10 processes messages including animated GIFs. A specially crafted chat message can cause an arbitrary file write, which could potentially be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to exploit this vulnerability.	Patch is available, please update the software.
Application: Openstack				
Potential Mistral Denial of Service handling recursive YAML anchor expansion	15-June-2020	**6.5 Medium**	**CVE-2018-16848** A Denial of Service (DoS) condition is possible in OpenStack Mistral in versions up to and including 7.0.3. Submitting a specially crafted workflow definition YAML file containing nested anchors can lead to resource exhaustion culminating in a denial of service.	https://bugzilla.redhat.com/show_bug.cgi?id=1645332 https://bugs.launchpad.net/mistral/+bug/1785657
Insecure-credentials flaw	10-June-2020	**6.5 Medium**	**CVE-2020-10755** An insecure-credentials flaw was found in all openstack-cinder versions before openstack-cinder 14.1.0, all openstack-cinder 15.x.x versions before openstack-cinder 15.2.0 and all openstack-cinder 16.x.x versions before openstack-cinder 16.1.0. When using openstack-cinder with the Dell EMC ScaleIO or VxFlex OS backend storage driver, credentials for the entire backend are exposed in the ``connection_info`` element in all Block Storage v3 Attachments API calls containing that element. This flaw enables an end-user to create a volume, make an API call to show the attachment detail information, and retrieve a username and password that	https://wiki.openstack.org/wiki/OSSN/OSSN-0086 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10755

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			may be used to connect to another user's volume. Additionally, these credentials are valid for the ScaleIO or VxFlex OS Management API, should an attacker discover the Management API endpoint. Source: OpenStack project	
Application: SQLite				
ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature.	27-May-2020	**7.0** **HIGH**	**CVE-2020-13630** ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature.	https://sqlite.org/src/info/0d69f76f0865f962
Application: Citrix				
Vulnerabilities in Citrix Workspace app and Receiver for Windows	11-June-2020	**7.8** **HIGH**	**CVE-2020-13884** **CVE-2020-13885** Vulnerabilities have been identified in Citrix Workspace app and Citrix Receiver for Windows that could result in a local user escalating their privilege level to administrator during the uninstallation process.	upgrade to Citrix Workspace app version 1912 or later. https://support.citrix.com/article/CTX275460
Application: Docker				
Docker Desktop	05-June-2020	**7.8** **HIGH**	**CVE-2020-11492** An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges.	https://docs.docker.com/docker-for-windows/release-notes/
Application: Netgear				
Unauthorized Remote Code Execution vulerability	29-May-2020	**8.3** **HIGH**	**CVE-2020-11549** **CVE-2020-11550** **CVE-2020-11551** NETGEAR has released fixes for an unauthorized remote code execution security vulnerability on the following product models: RBS50Y running firmware versions prior to 2.5.2.104	https://kb.netgear.com/000061905/Security-Advisory-for-Unauthorized-Remote-Code-Execution-on-Some-Orbi-Routers-and-Satellites-PSV-2020-0025

CV Scoring Scale (CVSS)	**0**	**0.1-3.9**	**4-6.9**	**7-8.9**	**9-10**
	None	**Low**	**Medium**	**High**	**Critical**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			SRR60 running firmware versions prior to 2.5.2.104 SRS60 running firmware versions prior to 2.5.2.104 NETGEAR strongly recommends that you download the latest firmware as soon as possible	
Application: Vim				
In Vim before 8.1.0881, users can circumvent the rvim restricted mode and execute arbitrary OS commands via scripting interfaces (e.g., Python, Ruby, or Lua).	28-May-2020	**5.3 Medium**	**CVE-2019-20807** In Vim before 8.1.0881, users can circumvent the rvim restricted mode and execute arbitrary OS commands via scripting interfaces (e.g., Python, Ruby, or Lua).	https://github.com/vim/vim/releases/tag/v8.1.0881 https://github.com/vim/vim/commit/8c62a08faf89663e5633dc5036cd8695c80f1075 http://lists.opensuse.org/opensuse-security-announce/2020-06/msg00018.html
Application: Apple				
Apple security updates			Apple Releases Security Updates Apple has released security updates to address vulnerabilities in multiple products.	Please visit following reference for more information: https://support.apple.com/en-us/HT201222 https://support.apple.com/HT211168 https://support.apple.com/HT211170 https://support.apple.com/HT211171 https://support.apple.com/HT211175 https://support.apple.com/HT211178 https://support.apple.com/HT211179 https://support.apple.com/HT211181

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical