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

Issue Date: 29-April-2020 **Issue Number:06**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Microsoft				
Remote code execution vulnerability	15-April-2020	**8.8 HIGH**	**CVE-2020-0966 & CVE-2020-0967** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0966 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0967
Remote code execution vulnerability	15-April-2020	**8.8 HIGH**	**CVE-2020-0906** A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0906
Remote code execution vulnerability	15-April-2020	**8.8 HIGH**	**CVE-2020-0687** A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0687
Remote code execution vulnerability	15-April-2020	**7.8 HIGH**	**CVE-2020-0889** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0889
Remote code execution vulnerability	15-April-2020	**7.8 HIGH**	**CVE-2020-0784 &CVE-2020-0888** An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0888

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0784
Remote code execution vulnerability	15-April-2020	**7.8 HIGH**	**CVE-2020-0961** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0961
Remote code execution vulnerability	15-April-2020	**7.5 HIGH**	**CVE-2020-0969** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0969
Remote code execution vulnerability	15-April-2020	**7.5 HIGH**	**CVE-2020-0970** A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0970
Remote code execution vulnerability	15-April-2020	**7.5 HIGH**	**CVE-2020-0968** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0968
Application: Cisco				
Cisco IP Phones Web Server Remote Code Execution and Denial of Service Vulnerability	15-April-2020	**9.8 CRITICAL**	**CVE-2020-3161** A vulnerability in the web server for Cisco IP Phones could allow an unauthenticated, remote attacker to execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web server of a targeted device. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phones-rce-dos-rB6EeRXs

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
			the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a DoS condition.	
Cisco IOS and Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability	28-April-2020	**8.8 HIGH**	**CVE-2019-16009** A vulnerability in the web UI of Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200108-ios-csrf
Multiple Vulnerabilities in Cisco UCS Director and Cisco UCS Director Express for Big Data	15-April-2020	**8.8 HIGH**	**CVE-2020-3239, CVE-2020-3240 & CVE-2020-3243** Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a remote attacker to bypass authentication or conduct directory traversal attacks on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsd-mult-vulns-UNfpdW4E
Cisco Wireless LAN Controller CAPWAP Denial of Service Vulnerability	15-April-2020	**8.6 HIGH**	**CVE-2020-3262** A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol handler of Cisco Wireless LAN Controller (WLC) 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-wlc-capwap-dos-Y2sD9uEw
Cisco Wireless LAN Controller 802.11 Generic Advertisement Service Denial of Service Vulnerability	15-April-2020	**8.6 HIGH**	**CVE-2020-3273** A vulnerability in the 802.11 Generic Advertisement Service (GAS) frame processing function of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS).	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-gas-dos-8FsE3AWH
Cisco Mobility Express Software Cross-Site Request Forgery Vulnerability	15-April-2020	**8.1 HIGH**	**CVE-2020-3261** A vulnerability in the web-based management interface of Cisco Mobility Express Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mob-exp-csrf-b8tFec24
Cisco Webex Network Recording Player and Cisco	15-April-2020	**7.8 HIGH**	**CVE-2020-3194** A vulnerability in Cisco Webex Network Recording Player for Microsoft	https://tools.cisco.com/security/center/content/CiscoSecuri

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
Webex Player Arbitrary Code Execution Vulnerability			Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system.	tyAdvisory/cisco-sa-webex-player-Q7Rtgvby
Cisco IP Phones Web Application Buffer Overflow Vulnerability	15-April-2020	**7.5 HIGH**	**CVE-2016-1421** A vulnerability in the web application for Cisco IP Phones could allow an unauthenticated, remote attacker to execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software fails to check the bounds of input data. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web server of a targeted device. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a DoS condition.	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160609-ipp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160609-ipp
Cisco IoT Field Network Director Denial of Service Vulnerability	15-April-2020	**7.5 HIGH**	**CVE-2020-3162** A vulnerability in the Constrained Application Protocol (CoAP) implementation of Cisco IoT Field Network Director 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-iot-coap-dos-WTBu6YTq
Cisco Unified Communications Manager Path Traversal Vulnerability	15-April-2020	**7.5 HIGH**	**CVE-2020-3177** A vulnerability in the Tool for Auto-Registered Phones Support (TAPS) of Cisco Unified Communications Manager (UCM) and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to conduct directory traversal attacks on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-taps-path-trav-pfsFO93r
Cisco Unified Contact Center Express Privilege Escalation Vulnerability	15-April-2020	**7.5 HIGH**	**CVE-2020-1888** A vulnerability in the Administration Web Interface of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to upload arbitrary files and execute commands on the underlying	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-privesc-Zd7bvwyf

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
			operating system. To exploit this vulnerability, an attacker needs valid Administrator credentials.	
Cisco Aironet Series Access Points Client Packet Processing Denial of Service Vulnerability	15-April-2020	**7.4 HIGH**	**CVE-2020-3260** A vulnerability in Cisco Aironet Series Access Points Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-airo-wpa-dos-5ZLs6ESz
Application: Apache				
Apache HTTPD: mod_proxy_ftp use of uninitialized value	1-April-2020	5.3 MEDIUM	**CVE-2020-1934** Apache HTTPD: mod_proxy_ftp use of uninitialized value	https://httpd.apache.org/security/vulnerabilities_24.html
Application: Apple				
Apple macOS Catalina vulnerability	1-April-2020	**9.8 CRITICAL**	**CVE-2020-3847** Apple macOS Catalina vulnerability An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to leak memory.	https://support.apple.com/HT210919
A memory corruption issue was addressed with improved input validation.	1-April-2020	**9.8 CRITICAL**	**CVE-2020-3848** A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	https://support.apple.com/HT210919
A memory corruption issue was addressed with improved input validation.	1-April-2020	**9.8 CRITICAL**	**CVE-2020-3850** A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	https://support.apple.com/HT210919
A memory corruption issue was addressed with	1-April-2020	**9.8 CRITICAL**	**CVE-2020-3849** A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS	https://support.apple.com/HT210919

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
improved input validation.			Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	
A buffer overflow was addressed with improved size validation.	1-April-2020	**9.8 CRITICAL**	**CVE-2020-3910** A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	https://support.apple.com/HT211100 https://support.apple.com/HT211101 https://support.apple.com/HT211102 https://support.apple.com/HT211103 https://support.apple.com/HT211105 https://support.apple.com/HT211106 https://support.apple.com/HT211107
A buffer overflow was addressed with improved bounds checking.	1-April-2020	**9.8 CRITICAL**	**CVE-2020-3911** A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	https://support.apple.com/HT211100 https://support.apple.com/HT211101 https://support.apple.com/HT211102 https://support.apple.com/HT211103 https://support.apple.com/HT211105 https://support.apple.com/HT211106 https://support.apple.com/HT211107
A buffer overflow was addressed with improved bounds checking.	1-April-2020	**9.8 CRITICAL**	**CVE-2020-3909** A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	https://support.apple.com/HT211100 https://support.apple.com/HT211101 https://support.apple.com/HT211102 https://support.apple.com/HT211103 https://support.apple.com/HT211105 https://support.apple.com/HT211106

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://support.apple.com/HT211107
A logic issue was addressed with improved state management	1-April-2020	**9.8 CRITICAL**	**CVE-2019-6203** A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. An attacker in a privileged network position may be able to intercept network traffic.	https://support.apple.com/HT209599 https://support.apple.com/HT209600 https://support.apple.com/HT209601
Multiple issues were addressed by updating to version 8.1.1850.	1-April-2020	**9.8 CRITICAL**	**CVE-2020-9769** Multiple issues were addressed by updating to version 8.1.1850. This issue is fixed in macOS Catalina 10.15.4. Multiple issues in Vim.	https://support.apple.com/HT211100
A use after free issue was addressed with improved memory management.	1-April-2020	**8.8 HIGH**	**CVE-2020-9783** A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution.	https://support.apple.com/HT211101 https://support.apple.com/HT211102 https://support.apple.com/HT211104 https://support.apple.com/HT211105 https://support.apple.com/HT211106 https://support.apple.com/HT211107
A type confusion issue was addressed with improved memory handling.	1-April-2020	**8.8 HIGH**	**CVE-2020-3901** A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/HT211101 https://support.apple.com/HT211102 https://support.apple.com/HT211103 https://support.apple.com/HT211104 https://support.apple.com/HT211105 https://support.apple.com/HT211106 https://support.apple.com/HT211107
Application: Huawei				
Buffer Overflow Vulnerability in	02-April-2020	**8.0 HIGH**	**CVE-2020-9067**	https://www.huawei.com/en/psirt/secu

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
Some Huawei Products			Buffer Overflow Vulnerability in Some Huawei Products There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include:SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800 versions V100R018C00, V100R018C10, V100R019C10.	rity-advisories/huawei-sa-20200401-01-overflow-en
Improper Authentication Vulnerability in Some Huawei Smartphones	26-MARCH-2020	**7.8 HIGH**	**CVE-2020-9066** Improper Authentication Vulnerability in Some Huawei Smartphones Huawei smartphones OxfordP-AN10B with versions earlier than 10.0.1.169(C00E166R4P1) have an improper authentication vulnerability. The Application doesn't perform proper authentication when user performs certain operations. An attacker can trick user into installing a malicious plug-in to exploit this vulnerability. Successful exploit could allow the attacker to bypass the authentication to perform unauthorized operations.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200325-01-phone
Application: Linux Kernel				
In the Linux kernel before 5.4.12, drivers/input/input.c has out-of-bounds writes via a crafted keycode table, as demonstrated by input_set_keycode, aka CID-cb222aed03d7.	08-April-2020	**9.8 CRITICAL**	**CVE-2019-20636** In the Linux kernel before 5.4.12, drivers/input/input.c has out-of-bounds writes via a crafted keycode table, as demonstrated by input_set_keycode, aka CID-cb222aed03d7.	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.4.12 https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=cb222aed03d798fc07

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
				4be55e59d9a112338ee784 https://github.com/torvalds/linux/commit/cb222aed03d798fc074be55e59d9a112338ee784 CVE-2020-11669
An issue was discovered in the Linux kernel before 5.2 on the powerpc platform.	10-APRIL-2020	**7.5 HIGH**	**CVE-2020-11669** An issue was discovered in the Linux kernel before 5.2 on the powerpc platform. arch/powerpc/kernel/idle_book3s.S does not have save/restore functionality for PNV_POWERSAVE_AMR, PNV_POWERSAVE_UAMOR, and PNV_POWERSAVE_AMOR, aka CID-53a712bae5dd.	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.2 https://access.redhat.com/errata/RHSA-2019:3517 http://lists.opensuse.org/opensuse-security-announce/2020-04/msg00035.html https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=53a712bae5dd919521a58d7bad773b949358add0 https://github.com/torvalds/linux/commit/53a712bae5dd919521a58d7bad773b949358add0
Application: F5 BIG-IP				
BIG-IP network failover vulnerability	27-MARCH-2020	**8.1 HIGH**	**CVE-2020-5860** BIG-IP network failover vulnerability On BIG-IP 15.0.0-15.1.0.2, 14.1.0-14.1.2.3, 13.1.0-13.1.3.2, 12.1.0-12.1.5.1, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, in a High Availability (HA) network failover in Device Service Cluster (DSC), the failover service does not require a strong form of authentication and HA network failover traffic is not encrypted by Transport Layer Security (TLS).	https://support.f5.com/csp/article/K67472032

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
BIG-IP AWS vulnerability	27-MARCH-2020	**7.5 HIGH**	**CVE-2020-5862** On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.2, under certain conditions, TMM may crash or stop processing new traffic with the DPDK/ENA driver on AWS systems while sending traffic. This issue does not affect any other platforms, hardware or virtual, or any other cloud provider since the affected driver is specific to AWS.	https://support.f5.com/csp/article/K01054113
BIG-IP HTTP/3 QUIC vulnerability	27-MARCH-2020	**7.5 HIGH**	**CVE-2020-5859** On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file.	https://support.f5.com/csp/article/K61367237
BIG-IP HTTP profile vulnerability	27-MARCH-2020	**7.5 HIGH**	**CVE-2020-5857** On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service.	https://support.f5.com/csp/article/K70275209
Application: Fortinet				
An external control of system vulnerability in FortiOS may allow an authenticated, regular user to change the routing settings of the device via connecting to the ZebOS component	02-April-2020	**8.8 HIGH**	**CVE-2018-13371** An external control of system vulnerability in FortiOS may allow an authenticated, regular user to change the routing settings of the device via connecting to the ZebOS component.	https://fortiguard.com/advisory/FG-IR-18-230
An Uncontrolled Resource Consumption vulnerability in Fortinet FortiSwitch below 3.6.11, 6.0.6 and 6.2.2, FortiAnalyzer below 6.2.3, FortiManager below 6.2.3 and	07-April-2020	**7.5 HIGH**	**CVE-2019-17657** An Uncontrolled Resource Consumption vulnerability in Fortinet FortiSwitch below 3.6.11, 6.0.6 and 6.2.2, FortiAnalyzer below 6.2.3, FortiManager below 6.2.3 and FortiAP-S/W2 below 6.2.2 may allow an attacker to cause admin webUI denial of service (DoS) via handling special crafted HTTP requests/responses in	https://fortiguard.com/psirt/FG-IR-19-013

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
FortiAP-S/W2 below 6.2.2			pieces slowly, as demonstrated by Slow HTTP DoS Attacks.	
An improper authorization vulnerability in FortiADC may allow a remote authenticated user with low privileges to perform certain actions such as rebooting the system.	07-APRIL-2020	**6.5 MEDIUM**	**CVE-2020-9286** An improper authorization vulnerability in FortiADC may allow a remote authenticated user with low privileges to perform certain actions such as rebooting the system.	https://fortiguard.com/psirt/FG-IR-20-013
Application: IBM				
IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17	31-MARCH-2020	**8.8 HIGH**	**CVE-2020-4238** IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 175411.	https://www.ibm.com/support/pages/node/6128949 https://exchange.xforce.ibmcloud.com/vulnerabilities/175411
IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17	31-MARCH-2020	**8.8 HIGH**	**CVE-2020-4237** IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 175410.	https://www.ibm.com/support/pages/node/6128943 https://exchange.xforce.ibmcloud.com/vulnerabilities/175410
IBM QRadar 7.3.0 to 7.3.3	15-APRIL-2020	**8.8 HIGH**	**CVE-2020-4272** IBM QRadar 7.3.0 to 7.3.3 Patch 2 could allow a remote attacker to include arbitrary files. A remote attacker could send a specially-crafted request specify a malicious file from a remote system, which could allow the attacker to execute arbitrary code on the vulnerable server. IBM X-ForceID: 175898.	https://www.ibm.com/support/pages/node/6189645 https://exchange.xforce.ibmcloud.com/vulnerabilities/175898
IBM QRadar 7.3.0 to 7.3.3	15-APRIL-2020	**7.8 HIGH**	**CVE-2020-4270** IBM QRadar 7.3.0 to 7.3.3 Patch 2 could allow a local user to gain	https://www.ibm.com/support/pages/node/6189657

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
			escalated privileges due to weak file permissions. IBM X-ForceID: 175846.	https://exchange.xforce.ibmcloud.com/vulnerabilities/175846
IBM MQ 9.0 and 9.1	16-APRIL-2020	**7.5 HIGH**	**CVE-2019-4762** IBM MQ 9.0 and 9.1 is vulnerable to a denial of service attack due to an error in the Channel processing function. IBM X-Force ID: 173625.	https://www.ibm.com/support/pages/node/4832931 https://exchange.xforce.ibmcloud.com/vulnerabilities/173625
IBM QRadar 7.3.0 to 7.3.3	16-APRIL-2020	**7.5 HIGH**	**CVE-2020-4269** IBM QRadar 7.3.0 to 7.3.3 Patch 2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-ForceID: 175845.	https://www.ibm.com/support/pages/node/6189711 https://exchange.xforce.ibmcloud.com/vulnerabilities/175845
IBM InfoSphere Information Server 11.3, 11.5, and 11.7	16-APRIL-2020	**7.3 HIGH**	**CVE-2020-4347** IBM InfoSphere Information Server 11.3, 11.5, and 11.7 could be subject to attacks based on privilege escalation due to inappropriate file permissions for files used by WebSphere Application Server Network Deployment. IBM X-Force ID: 178412.	https://www.ibm.com/support/pages/node/6191679 https://exchange.xforce.ibmcloud.com/vulnerabilities/178412
IBM QRadar 7.3.0 to 7.3.3	15-APRIL-2020	**5.9 MEDIUM**	**CVE-2019-4594** IBM QRadar 7.3.0 to 7.3.3 Patch 2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-ForceID: 167810.	https://www.ibm.com/support/pages/node/6189735 https://exchange.xforce.ibmcloud.com/vulnerabilities/167810
IBM Maximo Asset Management 7.6	17-APRIL-2020	**5.4 MEDIUM**	**CVE-2019-4446** IBM Maximo Asset Management 7.6 could allow an authenticated user perform actions they are not	https://www.ibm.com/support/pages/node/6190215 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
			authorized to by modifying request parameters. IBM X-Force ID: 163490.	vulnerabilities/163490
Application: Juniper				
Junos OS Evolved: Local log files accessible from the shell may leak sensitive information	08-APRIL-2020	**5.5 MEDIUM**	CVE-2020-1620 CVE-2020-1621 CVE-2020-1622 CVE-2020-1623 CVE-2020-1624 Multiple information disclosure vulnerabilities in Juniper Networks Junos OS Evolved allow a local, authenticated user with shell access the ability to view sensitive configuration information, such as the hashed values of login passwords and shared secrets. The information provided is similar to the output from 'show config system login', which is typically restricted to the super-user class. The log files are readable by any authenticated user with shell access. One or more of these issues affect all versions of Junos OS Evolved prior to 19.3R1.	https://kb.juniper.net/JSA11003
Application: Palo Alto				
An issue was discovered in Pulse Secure Pulse Connect Secure (PCS	06-APRIL-2020	**8.8 HIGH**	**CVE-2020-11582** An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, launches a TCP server that accepts local connections on a random port. This can be reached by local HTTP clients, because up to 25 invalid lines are ignored, and because DNS rebinding can occur.	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426
An insecure temporary file vulnerability in Palo Alto Networks Traps allows a local authenticated	08-APRIL-2020	**7.1 HIGH**	**CVE-2020-1991** An insecure temporary file vulnerability in Palo Alto Networks Traps allows a local authenticated Windows user to escalate privileges or overwrite system files. This issue	https://security.paloaltonetworks.com/CVE-2020-1991

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
Windows user to escalate privileges or overwrite system files			affects Palo Alto Networks Traps 5.0 versions before 5.0.8; 6.1 versions before 6.1.4 on Windows. This issue does not affect Cortex XDR 7.0. This issue does not affect Traps for Linux or MacOS.	
Application: Wordpress				
An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress.	01-April-2020	**9.8 CRITICAL**	**CVE-2020-7947** An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. It has numerous fields that can contain data that is pulled from different sources. One issue with this is that the data isn't sanitized, and no input validation is performed, before the exporting of the user data. This can lead to (at least) CSV injection if a crafted Excel document is uploaded.	https://wordpress.org/plugins/auth0/#developers https://auth0.com/docs/cms/wordpress
LifterLMS Wordpress plugin version below 3.37.15 is vulnerable to arbitrary file write leading to remote code execution	31-MARCH-2020	**9.8 CRITICAL**	**CVE-2020-6008** LifterLMS Wordpress plugin version below 3.37.15 is vulnerable to arbitrary file write leading to remote code execution	https://wordpress.org/plugins/lifterlms/#developers
LearnDash Wordpress plugin version below 3.1.6 is vulnerable to Unauthenticated SQL Injection.	01-April-2020	**9.8 CRITICAL**	**CVE-2020-6009** LearnDash Wordpress plugin version below 3.1.6 is vulnerable to Unauthenticated SQL Injection.	https://learndash.releasenotes.io/release/YBfaq-version-316
An issue was discovered in the Responsive Poll through 1.3.4 for Wordpress.	13-April-2020	**9.8 CRITICAL**	**CVE-2020-11673** An issue was discovered in the Responsive Poll through 1.3.4 for Wordpress. It allows an unauthenticated user to manipulate polls, e.g., delete, clone, or view a hidden poll. This is due to the usage of the callback wp_ajax_nopriv function in Includes/Total-Soft-Poll-Ajax.php for sensitive operations.	https://wordpress.org/plugins/poll-wp/#developers
The Snap Creek Duplicator plugin before 1.3.28 for	13-APRIL-2020	**7.5 HIGH**	**CVE-2020-11738** The Snap Creek Duplicator plugin before 1.3.28 for WordPress (and	https://snapcreek.com/duplicator/docs/changelog/?lite

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

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
WordPress (and Duplicator Pro before 3.8.7.1)			Duplicator Pro before 3.8.7.1) allows Directory Traversal via ../ in the file parameter to duplicator_download or duplicator_init.	
The Media Library Assistant plugin before 2.82 for Wordpress suffers from a Local File Inclusion vulnerability in mla_gallery link=download.	12-APRIL-2020	**7.5 HIGH**	**CVE-2020-11732** The Media Library Assistant plugin before 2.82 for Wordpress suffers from a Local File Inclusion vulnerability in mla_gallery link=download.	https://wordpress.org/plugins/media-library-assistant/#developers
Application: Zoom				
Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation	01-APRIL-2020	**7.8 HIGH**	**CVE-2020-11469** Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation, which allows a local process (with the user's privileges) to obtain root access by replacing runwithroot.	https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.	03-APRIL-2020	**7.5 HIGH**	**CVE-2020-11500** Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.	-
Application: Oracle				
Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware	15-April-2020	**9.8 CRITICAL**	**CVE-2020-2950** Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition.	https://www.oracle.com/security-alerts/cpuapr2020.html

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
			Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition.	
Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware	15-April-2020	**9.8 CRITICAL**	**CVE-2020-2915** Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Caching, CacheStore, Invocation). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence.	https://www.oracle.com/security-alerts/cpuapr2020.html
Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager	15-April-2020	**9.8 CRITICAL**	**CVE-2020-2961** Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Discovery Framework (Oracle OHS)). Supported versions that are affected are 13.2.0.0 and 13.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Enterprise Manager Base Platform.	https://www.oracle.com/security-alerts/cpuapr2020.html
Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards	15-April-2020	**9.8 CRITICAL**	**CVE-2020-2733** Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Monitoring and Diagnostics). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools.	https://www.oracle.com/security-alerts/cpuapr2020.html

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
Vulnerability in the Oracle Knowledge product of Oracle Knowledge	15-April-2020	**9.8 CRITICAL**	**CVE-2020-2791** Vulnerability in the Oracle Knowledge product of Oracle Knowledge (component: Information Manager Console). Supported versions that are affected are 8.6.0-8.6.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks of this vulnerability can result in takeover of Oracle Knowledge.	https://www.oracle.com/security-alerts/cpuapr2020.html
Vulnerability in the Oracle Solaris product of Oracle Systems	15-April-2020	**9.8 CRITICAL**	**CVE-2020-2944** Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris.	https://www.oracle.com/security-alerts/cpuapr2020.html
Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware	15-APRIL-2020	**8.8 HIGH**	**CVE-2020-2884** Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	https://www.oracle.com/security-alerts/cpuapr2020.html
Vulnerability in the Oracle Outside In Technology product	15-APRIL-2020	**7.3 HIGH**	**CVE-2020-2786** Vulnerability in the Oracle Outside In Technology product of Oracle Fusion	https://www.oracle.com/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
of Oracle Fusion Middleware			Middleware (component: Outside In Filters). Supported versions that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower.	alerts/cpuapr2020.html
Vulnerability in the MySQL Server product of Oracle MySQL	15-APRIL-2020	**5.9 MEDIUM**	**CVE-2020-2804** Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server	https://www.oracle.com/security-alerts/cpuapr2020.html
Application: Avast				
An issue was discovered in Avast Antivirus before 20	15-April-2020	**9.8 CRITICAL**	**CVE-2020-10867** An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows	https://forum.avast.com/index.php?topic=232423.0

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
			attackers to bypass intended access restrictions on tasks from an untrusted process, when Self Defense is enabled.	https://forum.avast.com/index.php?topic=232420.0
Application: Avira				
An issue was discovered in Avira Free-Antivirus before 15.0.2004.1825.	09-April-2020	**9.8 CRITICAL**	**CVE-2020-8961** An issue was discovered in Avira Free-Antivirus before 15.0.2004.1825. The Self-Protection feature does not prohibit a write operation from an external process. Thus, code injection can be used to turn off this feature. After that, one can construct an event that will modify a file at a specific location, and pass this event to the driver, thereby defeating the anti-virus functionality.	https://support.avira.com/hc/en-us/articles/360000109798-Avira-Antivirus-for-Windows
Application: ORTS				
An attacker with the ability to generate session IDs or password reset tokens, either by being able to authenticate or by exploiting OSA-2020-09	27-APRIL-2020	**8.1 HIGH**	**CVE-2020-1773** An attacker with the ability to generate session IDs or password reset tokens, either by being able to authenticate or by exploiting OSA-2020-09, may be able to predict other users session IDs, password reset tokens and automatically generated passwords. This issue affects ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS; 7.0.15 and prior versions.	https://otrs.com/release-notes/otrs-security-advisory-2020-10/
Application: XIAOMI				
An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.58.10.	08-APRIL-2020	**6.8 MEDIUM**	**CVE-2020-10262** An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.58.10. Attackers can activate the failsafe mode during the boot process, and use the mi_console command cascaded by the SN code shown on the product to get the root shell password, and then the attacker can (i) read Wi-Fi SSID or password, (ii) read the dialogue text files between users and XIAOMI XIAOAI speaker Pro LX06, (iii) use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, (iv) eavesdrop on users and	https://sec.xiaomi.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
			record what XIAOMI XIAOAI speaker Pro LX06 hears, (v) modify system files, (vi) use commands to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro (LX06), (vii) stop voice assistant service, (viii) enable the XIAOMI XIAOAI Speaker Pro's SSH or TELNET service as a backdoor, (IX) tamper with the router configuration of the router in the local area networks.	
Application: OpenSSL				
Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake	21-APRIL-2020	**HIGH**	**CVE-2020-1967** **CVE-2020-6459** **CVE-2020-6460** **CVE-2020-6458** Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack.	ttps://www.openssl.org/news/secadv/20200421.txt

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