BGD e-GOV CIRT

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

Issue Date: 28-November-2019 **Issue Number:01**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: sudo				
Sudo Local Privilege Escalation Vulnerability	16-OCT-2019	**8.8 HIGH**	**CVE-2019-14287** In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#$((0xffffffff))" command.	**sudo 1.8.28.** https://www.sudo.ws/alerts/minus_1_uid.html
Application: Exim message transfer				
Unauthenticated remote code execution vulnerability in the Exim message transfer agent	06-SEP-2019	**9.8 CRITICAL**	**CVE-2019-15846** Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash.	**exim-4.92.2** http://exim.org/static/doc/security/CVE-2019-15846.txt
Application: Wordpress Server-Side Request Forgery (SSRF)				
Server-Side Request Forgery (SSRF)	17-OCT-2019	**9.8 CRITICAL**	**CVE-2019-17669** WordPress before 5.2.4 has a Server Side Request Forgery (SSRF) vulnerability because URL validation does not consider the interpretation of a name as a series of hex characters.	**WordPress 5.2.4** https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
Application: PuTTY				
PuTTY vulnerability	01-OCT-2019	**9.8 CRITICAL**	PuTTY before 0.73 on Windows improperly opens port-forwarding listening sockets, which allows attackers to listen on the same port to steal an incoming connection.	**PuTTY 0.73** https://lists.tartarus.org/pipermail/putty-announce/2019/000029.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
Application: Microsoft Azure App Service Remote Code Execution				
Azure App Service Remote Code Execution Vulnerability	10-OCT-2019	**10 CRITICAL**	**CVE-2019-1372** An remote code execution vulnerability exists when Azure App Service/ Antares on Azure Stack fails to check the length of a buffer prior to copying memory to it.An attacker who successfully exploited this vulnerability could allow an unprivileged function run by the user to execute code in the context of NT AUTHORITY\system thereby escaping the Sandbox.The security update addresses the vulnerability by ensuring that Azure App Service sanitizes user inputs., aka 'Azure App Service Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1372
Application: MS XML Remote Code Execution				
MS XML Remote Code Execution Vulnerability	10-OCT-2019	**8.8 HIGH**	**CVE-2019-1060** A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-106
Application: Microsoft Windows Remote Desktop Client Remote Code Execution				
Remote Desktop Client Remote Code Execution Vulnerability	10-OCT-2019	**8.8 HIGH**	**CVE-2019-1333** A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1333
Application: Microsoft VBScript Remote Code Execution				
VBScript Remote Code Execution Vulnerability	10-OCT-2019	**7.5 HIGH**	**CVE-2019-1238, CVE-2019-1239** 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-2019-1238 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1239

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: Microsoft Edge				
Chakra Scripting Engine Memory Corruption Vulnerability	10-OCT-2019	**7.5 HIGH**	**CVE-2019-1307, CVE-2019-1308, CVE-2019-1335, CVE-2019-1366** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1307 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1308 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1335 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1366
Application: Microsoft SQL Server				
SQL Server Management Studio Information Disclosure Vulnerability	10-OCT-2019	**6.5 Medium**	**CVE-2019-1313, CVE-2019-1376** An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1313 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1376
Application: Microsoft Windows				
Windows NTLM Tampering Vulnerability	10-OCT-2019	**5.9 Medium**	**CVE-2019-1166** A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1166

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: Cisco Firepower Management Center				
Cisco Firepower Management Center SQL Injection Vulnerabilities	02-OCT-2019	**8.8 HIGH**	**CVE-2019-12679, CVE-2019-12680, CVE-2019-12681, CVE-2019-12682, CVE-2019-12683, CVE-2019-12684, CVE-2019-12685, CVE-2019-12686** Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-sql-inj
Cisco Firepower Management Center Remote Code Execution Vulnerability	02-OCT-2019	**8.8 HIGH**	**CVE-2019-12687, CVE-2019-12688** A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to execute arbitrary commands within the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce
Cisco Firepower Management Center Command Injection Vulnerability	02-OCT-2019	**7.2 HIGH**	**CVE-2019-12690** A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to inject arbitrary commands that are executed with the privileges of the root user of the underlying operating system. The vulnerability is due to insufficient	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-com-inj

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
			validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by submitting crafted input in the web UI. A successful exploit could allow an attacker to execute arbitrary commands on the device with full root privileges.	
Application: cPanel API				
cPanel up to 82.0.14 API Token weak authentication	09-OCT-2019	**8.8 HIGH**	**CVE-2019-17375** cPanel before 82.0.15 allows API token credentials to persist after an account has been renamed or terminated (SEC-517).	**cPane build 11.82.0.15.** https://news.cpanel.com/cpanel-tsr-2019-0005-full-disclosure/
Application: Joomla				
Shack Forms Pro Extension up to 4.0.31 on Joomla file attachment directory traversal	09-OCT-2019	**9.8 CRITICAL**	**CVE-2019-17399** The Shack Forms Pro extension before 4.0.32 for Joomla! allows path traversal via a file attachment.	**Upgrading to version 4.0.32.** https://www.joomlashack.com/changelog/shack-forms/
Application: D-Link DIR-846				
D-Link DIR-846 100A35 privilege escalation	11-OCT-2019	**9.8 CRITICAL**	**CVE-2019-17509, CVE-2019-17510** D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access	-
Application: Oracle Database Server				
Vulnerability in the Java VM component of Oracle Database Server.	16-OCT-2019	**6.8 Medium**	**CVE-2019-2909** Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java VM. While the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data.	http://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.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 Core RDBMS (jackson-databind) component of Oracle Database Server.	16-OCT-2019	**5.7 Medium**	**CVE-2019-2956** Vulnerability in the Core RDBMS (jackson-databind) component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via multiple protocols to compromise Core RDBMS (jackson-databind). Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Core RDBMS (jackson-databind).	http://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html
Vulnerability in the Core RDBMS (jackson-databind) component of Oracle Database Server.	16-OCT-2019	**5.0 Medium**	**CVE-2019-2913** Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via OracleNet to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS accessible data.	http://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html
Application: Google Android				
Google Android 8.0/8.1/9.0/10 NFC Application Vulnerability	11-OCT-2019	**5.5 Meium**	**CVE-2019-2114, CVE-2019-2187** In nfc_ncif_decode_rf_params of nfc_ncif.cc, there is a possible out of bounds read due to an integer underflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-124940143	https://source.android.com/security/bulletin/2019-10-01

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: Linux Kernel				
Linux Kernel up to 5.2.17 Beacon Head net/wireless/NL80211.C validate_beacon_head memory corruption	24-SEP-2019	**9.8 CRITICAL**	**CVE-2019-16746** An issue was discovered in net/wireless/nl80211.c in the Linux kernel through 5.2.17. It does not check the length of variable elements in a beacon head, leading to a buffer overflow.	https://marc.info/?l=linux-wireless&m=156901391225058&w=2
Linux Kernel up to 5.3.2 SSID net/wireless/wext-sme.c cfg80211_mgd_wext_giwessid memory corruption	04-OCT-2019	**9.8 CRITICAL**	**CVE-2019-17133** In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow.	https://marc.info/?l=linux-wireless&m=157018270915487&w=2
Linux Kernel up to 5.3.6 ps.c rtl_p2p_noa_ie memory corruption	16-OCT-2019	**8.8 High**	**CVE-2019-17666** rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel through 5.3.6 lacks a certain upper-bound check, leading to a buffer overflow.	-
Linux Kernel up to 5.3.2 cxgb4 Driver mem.c write_tpt_entry denial of service	01-OCT-2019	**7.5 High**	**CVE-2019-17075** An issue was discovered in write_tpt_entry in drivers/infiniband/hw/cxgb4/mem.c in the Linux kernel through 5.3.2. The cxgb4 driver is directly calling dma_map_single (a DMA function) from a stack variable. This could allow an attacker to trigger a Denial of Service, exploitable if this driver is used on an architecture for which this stack/DMA interaction has security relevance.	https://lore.kernel.org/lkml/20191001165611.GA3542072@kroah.com

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