**Issue Date: 01-April-2020 Issue Number:05**

 **BGD e-GOV CIRT project**

**Common Vulnerabilities and Exposures (CVE) Report**

| **Vulnerability** | **Publish Date** | **CSVV** | **CVE ID & Description** | **Patch** |
| --- | --- | --- | --- | --- |
| **Application: Microsoft** | | | | |
| GDI+ Remote Code Execution Vulnerability | 10-MARCH-2020 | **8.8**  **HIGH** | **CVE-2020-0881, CVE-2020-0883**  A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0881  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0883 |
| LNK Remote Code Execution Vulnerability | 10-MARCH-2020 | **8.8**  **HIGH** | **CVE-2020-0684**  A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a LNK file is processed. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0684 |
| Microsoft Edge Memory Corruption Vulnerability | 10-MARCH-2020 | **8.8**  **HIGH** | **CVE-2020-0816**  A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0816 |
| Dynamics Business Central Remote Code Execution Vulnerability | 10-MARCH-2020 | **8.0**  **HIGH** | **CVE-2020-0905**  An remote code execution vulnerability exists in Microsoft Dynamics Business Central, aka 'Dynamics Business Central Remote Code Execution Vulnerability'. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0905 |
| Win32k Elevation of Privilege Vulnerability | 10-MARCH-2020 | **7.8**  **HIGH** | **CVE-2020-0788**  **CVE-2020-0877**  **CVE-2020-0887**  An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0788  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0877  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0887 |
| Microsoft IIS Server Tampering Vulnerability | 10-MARCH-2020 | **7.5**  **HIGH** | **CVE-2020-0645**  A tampering vulnerability exists when Microsoft IIS Server improperly handles malformed request headers, aka 'Microsoft IIS Server Tampering Vulnerability'. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0645 |
| Chakra Scripting Engine Memory Corruption Vulnerability | 10-MARCH-2020 | **7.5**  **HIGH** | **CVE-2020-0811, CVE-2020-0812**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based) L, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0811  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0812 |
| Scripting Engine Memory Corruption Vulnerability | 10-MARCH-2020 | **7.5**  **HIGH** | **CVE-2020-0768**  **CVE-2020-0830**  A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0768  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0830 |
| Scripting Engine Memory Corruption Vulnerability | 10-MARCH-2020 | **7.5**  **HIGH** | **CVE-2020-0823**  **CVE-2020-0825**  **CVE-2020-0826**  **CVE-2020-0827**  **CVE-2020-0828**  **CVE-2020-0829**  **CVE-2020-0831**  **CVE-2020-0832**  **CVE-2020-0833**  **CVE-2020-0848**  A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0823  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0825  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0826  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0827  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0828  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0829  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0831  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0832  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0833  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0848 |
| Internet Explorer Memory Corruption Vulnerability | 10-MARCH-2020 | **7.5**  **HIGH** | **CVE-2020-0824**  A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0824 |
| VBScript Remote Code Execution Vulnerability | 10-MARCH-2020 | **7.5**  **HIGH** | **CVE-2020-0847**  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-2020-0847 |
| Azure DevOps Elevation of Privilege Vulnerability | 10-MARCH-2020 | **7.5**  **HIGH** | **CVE-2020-0758**  **CVE-2020-0815**  An elevation of privilege vulnerability exists when Azure DevOps Server and Team Foundation Services improperly handle pipeline job tokens. An attacker who successfully exploited this vulnerability could extend their access to a project. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0758  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0815 |
| Remote Desktop Connection Manager Information Disclosure Vulnerability | 10-MARCH-2020 | **5.5 MEDIUM** | **CVE-2020-0765**  An information disclosure vulnerability exists in the Remote Desktop Connection Manager (RDCMan) application when it improperly parses XML input containing a reference to an external entity, aka 'Remote Desktop Connection Manager Information Disclosure Vulnerability'. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0765 |
| Microsoft Exchange Server Spoofing Vulnerability | 10-MARCH-2020 | **5.4 MEDIUM** | **CVE-2020-0903**  A cross-site-scripting (XSS) vulnerability exists when Microsoft Exchange Server does not properly sanitize a specially crafted web request to an affected Exchange server, aka 'Microsoft Exchange Server Spoofing Vulnerability'. | https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0903 |
| **Application: Centos** | | | | |
| Centos WebPanel 7 - 'term' SQL Injection | 13-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-10230**  CentOS-WebPanel.com (aka CWP) CentOS Web Panel (for CentOS 6 and 7) allows SQL Injection via the /cwp\_{SESSION\_HASH}/admin/loader\_ajax.php term parameter. | https://centos-webpanel.com/changelog-cwp7 |
| **Application: cPanel** | | | | |
| cPanel before 84.0.20 allows a demo account to achieve remote code execution via a cpsrvd rsync shell (SEC-544). | 17-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-10119**  cPanel before 84.0.20 allows a demo account to achieve remote code execution via a cpsrvd rsync shell (SEC-544). | https://documentation.cpanel.net/display/CL/84+Change+Log |
| cPanel before 82.0.18 allows WebDAV authentication bypass because the connection-sharing logic is incorrect (SEC-534). | 17-MARCH-2020 | **9.8 CRITICAL** | **CVE-2019-2049**  cPanel before 82.0.18 allows WebDAV authentication bypass because the connection-sharing logic is incorrect (SEC-534). | https://documentation.cpanel.net/display/CL/82+Change+Log |
| cPanel before 84.0.20, when PowerDNS is used, allows arbitrary code execution as root via dnsadmin. (SEC-537). | 17-MARCH-2020 | **7.2**  **HIGH** | **CVE-2020-10115**  cPanel before 84.0.20, when PowerDNS is used, allows arbitrary code execution as root via dnsadmin. (SEC-537). | https://documentation.cpanel.net/display/CL/84+Change+Log |
| cPanel before 84.0.20 allows resellers to achieve remote code execution as root via a cpsrvd rsync shell (SEC-545). | 17-MARCH-2020 | **7.2**  **HIGH** | **CVE-2020-1012**  cPanel before 84.0.20 allows resellers to achieve remote code execution as root via a cpsrvd rsync shell (SEC-545). | https://documentation.cpanel.net/display/CL/84+Change+Log |
| **Application: Apache** | | | | |
| Apache Commons Configuration uses a third-party library to parse YAML files | 13-MARCH-2020 | **10.0 CRITICAL** | **CVE-2020-1953**  Apache Commons Configuration uses a third-party library to parse YAML files which by default allows the instantiation of classes if the YAML includes special statements. Apache Commons Configuration versions 2.2, 2.3, 2.4, 2.5, 2.6 did not change the default settings of this library. So if a YAML file was loaded from an untrusted source, it could therefore load and execute code out of the control of the host application. | https://lists.apache.org/thread.html/rde2186ad6ac0d6ed8d51af7509244adcf1ce0f9a3b7e1d1dd3b64676@%3Ccommits.camel.apache.org%3E |
| Apache Sharding Sphere(incubator) 4.0.0-RC3 and 4.0.0 | 11-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-1947**  In Apache ShardingSphere(incubator) 4.0.0-RC3 and 4.0.0, the ShardingSphere's web console uses the SnakeYAML library for parsing YAML inputs to load datasource configuration. SnakeYAML allows to unmarshal data to a Java type By using the YAML tag. Unmarshalling untrusted data can lead to security flaws of RCE. | https://lists.apache.org/thread.html/r4a61a24c119bd820da6fb02100d286f8aae55c8f9b94a346b9bb27d8%40%3Cdev.shardingsphere.apache.org%3E |
| FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.hadoop.shaded.com.zaxxer.hikari.HikariConfig (aka shaded hikari-config). | 01-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-9546**  FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.hadoop.shaded.com.zaxxer.hikari.HikariConfig (aka shaded hikari-config). | https://github.com/FasterXML/jackson-databind/issues/2631  https://lists.apache.org/thread.html/r35d30db00440ef63b791c4b7f7acb036e14d4a23afa2a249cb66c0fd@<issues.zookeeper.apache.org>  https://lists.apache.org/thread.html/r893a0104e50c1c2559eb9a5812add28ae8c3e5f43712947a9847ec18@%3Cnotifications.zookeeper.apache.org%3E  https://lists.apache.org/thread.html/rdd49ab9565bec436a896bc00c4b9fc9dce1598e106c318524fbdfec6@%3Cissues.zookeeper.apache.org%3E  https://lists.debian.org/debian-lts-announce/2020/03/msg00008.html |
| **Application: Draytek** | | | | |
| Vigor3900 / Vigor2960 / Vigor300B Router Web Management Page Vulnerability | 10-FEB-2020 | **9.8 CRITICAL** | **CVE-2020-8515**  DrayTek Vigor2960 1.3.1\_Beta, Vigor3900 1.4.4\_Beta, and Vigor300B 1.3.3\_Beta, 1.4.2.1\_Beta, and 1.4.4\_Beta devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI. This issue has been fixed in Vigor3900/2960/300B v1.5.1. | https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-(cve-2020-8515)/ |
| **Application: Liferay Portal** | | | | |
| Unauthenticated Remote code execution via JSONWS | 20-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-7961**  Deserialization of Untrusted Data in Liferay Portal prior to 7.2.1 CE GA2 allows remote attackers to execute arbitrary code via JSON web services (JSONWS). | https://portal.liferay.dev/learn/security/known-vulnerabilities  https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset\_publisher/HbL5mxmVrnXW/content/id/117954271 |
| **Application: Adobe** | | | | |
| Adobe Security Bulletin | 25-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-3790**  **CVE-2020-3789**  **CVE-2020-3788**  **CVE-2020-3787**  **CVE-2020-3786**  **CVE-2020-3785**  **CVE-2020-3784**  **CVE-2020-3783**  Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. | https://helpx.adobe.com/security/products/photoshop/apsb20-14.html |
| **Application: Samsung Mobile Devices** | | | | |
| Samsung mobile devices with P(9.0) devices (Qualcomm chipsets) software | 24-MARCH-2020 | **9.8 CRITICAL** | **CVE-2019-20548**  An issue was discovered on Samsung mobile devices with P (9.0) devices (Qualcomm chipsets) software. There is a buffer overflow in the bootloader. The Samsung ID is SVE-2019-15399 (November 2019). | https://security.samsungmobile.com/securityUpdate.smsb |
| Samsung mobile devices with P(9.0) (TEEGRIS and Qualcomm chipsets). | 24-MARCH-2020 | **9.8 CRITICAL** | **CVE-2019-20537**  An issue was discovered on Samsung mobile devices with P (9.0) (TEEGRIS and Qualcomm chipsets). There is arbitrary memory overwrite in the SEM Trustlet, leading to arbitrary code execution. The Samsung IDs are SVE-2019-14651, SVE-2019-14666 (November 2019). | https://security.samsungmobile.com/securityUpdate.smsb |
| Samsung mobile devices with N(7.x), O(8.0), and P(9.0) (Qualcomm chipsets) software | 24-MARCH-2020 | **7.5 HIGH** | **CVE-2019-20602**  An issue was discovered on Samsung mobile devices with N (7.x), O(8.0), and P(9.0) (Qualcomm chipsets) software. The Authnr Trustlet has a NULL pointer dereference. The Samsung ID is SVE-2019-13949 (May 2019). | https://security.samsungmobile.com/securityUpdate.smsb |
| **Application: Kyocera printers** | | | | |
| Multiple Buffer Overflows in Web Server | 13-MARCH-2020 | **9.8 CRITICAL** | **Multiple Buffer Overflows in Web Server (CVE-2019-13196, CVE-2019-13197, CVE-2019-13202, CVE-2019-13203, CVE-2019-13206)**  Some Kyocera printers were affected by several buffer overflow vulnerabilities in the web application that would allow an attacker to perform a Denial of Service attack, and potentially execute arbitrary code on the device. | - |
| **Application: Wordpress** | | | | |
| An issue was discovered in the File Upload plugin before 4.13.0 for WordPress | 13-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-10564**  An issue was discovered in the File Upload plugin before 4.13.0 for WordPress. A directory traversal can lead to remote code execution by uploading a crafted txt file into the lib directory, because of a wfu\_include\_lib call. | https://wordpress.org/plugins/wp-file-upload/#developers |
| controllers/quizzes.php in the Kiboko Chained Quiz plugin before 1.0.9 for WordPress | 10-MARCH-2020 | **9.8 CRITICAL** | **CVE-2018-14502**  controllers/quizzes.php in the Kiboko Chained Quiz plugin before 1.0.9 for WordPress allows remote unauthenticated users to execute arbitrary SQL commands via the 'answer' and 'answers' parameters. | https://wordpress.org/plugins/chained-quiz/#developers |
| The Registration Magic plugin through 4.6.0.3 for WordPress allows remote authenticated users | 06-MARCH-2020 | **8.8 HIGH** | **CVE-2020-9457**  The Registration Magic plugin through 4.6.0.3 for WordPress allows remote authenticated users (with minimal privileges) to import custom vulnerable forms and change form settings via class\_rm\_form\_settings\_controller.php, resulting in privilege escalation. | https://wordpress.org/plugins/custom-registration-form-builder-with-submission-manager/#developers |
| In the RegistrationMagic plugin through 4.6.0.3 for WordPress, the user controller allows remote authenticated users | 06-MARCH-2020 | **8.8 HIGH** | **CVE-2020-9456**  In the RegistrationMagic plugin through 4.6.0.3 for WordPress, the user controller allows remote authenticated users (with minimal privileges) to elevate their privileges to administrator via class\_rm\_user\_controller.php rm\_user\_edit. | https://wordpress.org/plugins/custom-registration-form-builder-with-submission-manager/#developers |
| A CSRF vulnerability in the Registration Magic plugin through 4.6.0.3 for WordPress allows remote attackers | 06-MARCH-2020 | **8.8 HIGH** | **CVE-2020-9454**  A CSRF vulnerability in the Registration Magic plugin through 4.6.0.3 for WordPress allows remote attackers to forge requests on behalf of a site administrator to change all settings for the plugin, including deleting users, creating new roles with escalated privileges, and allowing PHP file uploads via forms. | https://wordpress.org/plugins/custom-registration-form-builder-with-submission-manager/#developers |
| The sitepress-multilingual-cms (WPML) plugin before 4.3.7-b.2 for WordPress has CSRF due to a loose comparison | 14-MARCH-2020 | **8.8 HIGH** | **CVE-2020-10568**  The sitepress-multilingual-cms (WPML) plugin before 4.3.7-b.2 for WordPress has CSRF due to a loose comparison. This leads to remote code execution in includes/class-wp-installer.php via a series of requests that leverage unintended comparisons of integers to strings. | - |
| **Application: VMware** | | | | |
| VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) | 16-MARCH-2020 | **8.8 HIGH** | **CVE-2020-3947**  VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition of the vmnetdhcp service running on the host machine. | https://www.vmware.com/security/advisories/VMSA-2020-0004.html |
| VMware Horizon Client for Windows (5.x and prior before 5.3.0), VMware Remote Console for Windows (10.x before 11.0.0), VMware Workstation for Windows (15.x before 15.5.2) | 16-MARCH-2020 | **7.8 HIGH** | **CVE-2019-5543**  For VMware Horizon Client for Windows (5.x and prior before 5.3.0), VMware Remote Console for Windows (10.x before 11.0.0), VMware Workstation for Windows (15.x before 15.5.2) the folder containing configuration files for the VMware USB arbitration service was found to be writable by all users. A local user on the system where the software is installed may exploit this issue to run commands as any user. | https://www.vmware.com/security/advisories/VMSA-2020-0004.html |
| **Application: Huawei** | | | | |
| Some Huawei products have a security vulnerability due to improper authentication | 20-MARCH-2020 | **8.1 HIGH** | **CVE-2020-1864**  Some Huawei products have a security vulnerability due to improper authentication. A remote attacker needs to obtain some information and forge the peer device to send specific packets to the affected device. Due to the improper implementation of the authentication function, attackers can exploit the vulnerability to connect to affected devices and execute a series of commands.Affected product versions include:Secospace AntiDDoS8000 versions V500R001C00,V500R001C20,V500R001C60,V500R005C00. | https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200318-01-authentication-en |
| Huawei USG6000V with versions V500R001C20SPC300, V500R003C00SPC100, and V500R005C00SPC100 | 12-MARCH-2020 | **7.5 HIGH** | **CVE-2020-1863**  Huawei USG6000V with versions V500R001C20SPC300, V500R003C00SPC100, and V500R005C00SPC100 have an out-of-bounds read vulnerability. Due to a logical flaw in a JSON parsing routine, a remote, unauthenticated attacker could exploit this vulnerability to disrupt service in the affected products. | https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200311-01-buffer-en |
| NIP6800; Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 | 28-FEB-2020 | **7.5 HIGH** | CVE-2020-1881  NIP6800; Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have have a resource management error vulnerability. An attacker needs to perform specific operations to trigger a function of the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause service abnormal on affected devices. | https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-02-resource-en |
| NIP6800; Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 | 28-FEB-2020 | **7.5 HIGH** | **CVE-2020-1873**  NIP6800; Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have an out-of-bounds read vulnerability. An unauthenticated attacker crafts malformed message with specific parameter and sends the message to the affected products. Due to insufficient validation of message, which may be exploited to cause the device reboot. | https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-01-outofboundread-en |
| **Application: Palo Alto** | | | | |
| A shell command injection vulnerability | 11-MARCH-2020 | **7.8 HIGH** | **CVE-2020-1980**  A shell command injection vulnerability in the PAN-OS CLI allows a local authenticated user to escape the restricted shell and escalate privileges. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions. This issue is fixed in PAN-OS 8.1.13, and all later versions. | https://security.paloaltonetworks.com/CVE-2020-1980 |
| A predictable temporary filename vulnerability in PAN-OS allows local privilege escalation. | 11-MARCH-2020 | **7.8 HIGH** | **CVE-2020-1981**  A predictable temporary filename vulnerability in PAN-OS allows local privilege escalation. This issue allows a local attacker who bypassed the restricted shell to execute commands as a low privileged user and gain root access on the PAN-OS hardware or virtual appliance. This issue affects only PAN-OS 8.1 versions earlier than PAN-OS 8.1.13. This issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later PAN-OS versions. | https://security.paloaltonetworks.com/CVE-2020-1981 |
| **Application: anttix\_linux\_and\_mx\_linux** | | | | |
| antiX and MX Linux allow local users to achieve root access via "persist-config --command /bin/sh" because of the Sudo configuration. | 14-MARCH-2020 | **7.8 HIGH** | **CVE-2020-10587**  antiX and MX Linux allow local users to achieve root access via "persist-config --command /bin/sh" because of the Sudo configuration. | - |
| **Application: Apple** | | | | |
| Apple iTunes security update for CVE-2019-8741 | 18-FEB-2020 | **7.8 HIGH** | **CVE-2019-8741**  A denial of service issue was addressed with improved input validation. | https://support.apple.com/HT210604  https://support.apple.com/HT210606  https://support.apple.com/HT210607  https://support.apple.com/HT210634  https://support.apple.com/HT210635  https://support.apple.com/HT210636  https://support.apple.com/HT210637 |
| **Application: Squid** | | | | |
| Squid before 4.9, when certain web browsers are used, mishandles HTML in the host (aka hostname) parameter to cachemgr.cgi. | 20-MARCH-2020 | **6.1 MEDIUM** | **CVE-2019-18860**  Squid before 4.9, when certain web browsers are used, mishandles HTML in the host (aka hostname) parameter to cachemgr.cgi. | https://github.com/squid-cache/squid/pull/504  https://github.com/squid-cache/squid/pull/505 |
| **Application: Lexmark** | | | | |
| Unrestricted Upload Lexmark Markvision Enterprise (MVE) before 2.4.1 | 09-MARCH-2020 | **9.8 CRITICAL** | **CVE-2016-6918**  Lexmark Markvision Enterprise (MVE) before 2.4.1 allows remote attackers to execute arbitrary commands by uploading files. | http://support.lexmark.com/index? HP |
| **Application: HP** | | | | |
| Improper Authentication of certain HP Printers | 16-MARCH-2020 | **9.8 CRITICAL** | **CVE-2019-18917**  A potential security vulnerability has been identified for certain HP Printers and All-in-Ones that would allow bypassing account lockout. | https://support.hp.com/us-en/document/c06594863page=content&id=TE828&locale=EN&userlocale=EN\_US |
| **Application: ESET** | | | | |
| ESET Smart Security Premium AV Parsing Engine Archive privilege escalation | 05-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-10180**  The ESET AV parsing engine allows virus-detection bypass via a crafted BZ2 Checksum field in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop. | Fixed in new version (v. 1296) of unpacker module.  https://support.eset.com/en/ca7387-modules-review-december-2019 |
| ESET Smart Security Premium Archive Support Module privilege escalation | 06-MARCH-2020 | **7.5 HIGH** | **CVE-2020-10193**  ESET Archive Support Module before 1294 allows virus-detection bypass via crafted RAR Compression Information in an archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop. | Fixed in new version (v. 1296) of unpacker module.  https://support.eset.com/en/ca7387-modules-review-december-2019 |
| **Application: Sophos** | | | | |
| Sophos HitmanPro.Alert up to Build 860 privilege escalation | 01-MARCH-2020 | **7.8 HIGH** | **CVE-2020-9540**  Sophos HitmanPro.Alert before build 861 allows local elevation of privilege. | https://www.hitmanpro.com/en-us/whatsnewalert.aspx |
| **Application: Trend Micro** | | | | |
| Trend Micro Apex One/OfficeScan XG EXE File privilege escalation | 17-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-8599**  Trend Micro Apex One (2019) and OfficeScan XG server contain a vulnerable EXE file that could allow a remote attacker to write arbitrary data to an arbitrary path on affected installations and bypass ROOT login. Authentication is not required to exploit this vulnerability. | https://success.trendmicro.com/jp/solution/000244253  https://success.trendmicro.com/solution/000245571 |
| Trend Micro Apex One DLL privilege escalation | 17-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-8598**  Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow a remote attacker to execute arbitrary code on affected installations with SYSTEM level privileges. Authentication is not required to exploit this vulnerability. | https://success.trendmicro.com/jp/solution/000244253  https://success.trendmicro.com/jp/solution/000244836  https://success.trendmicro.com/solution/000245571  https://success.trendmicro.com/solution/000245572 |
| Trend Micro Apex One DLL denial of service | 17-MARCH-2020 | **7.5 HIGH** | **CVE-2020-8470**  Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow an attacker to delete any file on the server with SYSTEM level privileges. Authentication is not required to exploit this vulnerability. | https://success.trendmicro.com/solution/000245572  https://success.trendmicro.com/solution/000245571  https://success.trendmicro.com/jp/solution/000244836  https://success.trendmicro.com/jp/solution/000244253 |
| **Application: urllib3** | | | | |
| Uncontrolled Resource Consumption | 06-MARCH-2020 | **7.5 HIGH** | **CVE-2020-7212**  The \_encode\_invalid\_chars function in util/url.py in the urllib3 library 1.25.2 through 1.25.7 for Python allows a denial of service (CPU consumption) because of an inefficient algorithm. The percent\_encodings array contains all matches of percent encodings. It is not deduplicated. For a URL of length N, the size of percent\_encodings may be up to O(N). The next step (normalize existing percent-encoded bytes) also takes up to O(N) for each step, so the total time is O(N^2). If percent\_encodings were deduplicated, the time to compute \_encode\_invalid\_chars would be O(kN), where k is at most 484 ((10+6\*2)^2). | https://pypi.org/project/urllib3/1.25.8/  https://github.com/urllib3/urllib3/blob/master/CHANGES.rst  https://github.com/urllib3/urllib3/commit/a74c9cfbaed9f811e7563cfc3dce894928e0221a |
| **Application: Wing FTP Server** | | | | |
| Improper Privilege Management of Wing FTP Server v6.2.3 | 06-MARCH-2020 | **7.8 HIGH** | **CVE-2020-8635**  Wing FTP Server v6.2.3 for Linux, macOS, and Solaris sets insecure permissions on installation directories and configuration files. This allows local users to arbitrarily create FTP users with full privileges, and escalate privileges within the operating system by modifying system files. | - |
| **Application: SUSE Linux** | | | | |
| Symlink Following vulnerability of SUSE Linux Enterprise Server 12 | 02-MARCH-2020 | **7.8 HIGH** | **CVE-2019-18897**  A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of salt of SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15; openSUSE Factory allows local attackers to escalate privileges from user salt to root. This issue affects: SUSE Linux Enterprise Server 12 salt-master version 2019.2.0-46.83.1 and prior versions. SUSE Linux Enterprise Server 15 salt-master version 2019.2.0-6.21.1 and prior versions. openSUSE Factory salt-master version 2019.2.2-3.1 and prior versions. | https://bugzilla.suse.com/show\_bug.cgi?id=1157465  http://lists.opensuse.org/opensuse-security-announce/2020-03/msg00026.html |
| **Application: Avast** | | | | |
| Avast AntiTrack before 1.5.1.172 and AVG Antitrack before 2.0.0.178 proxies traffic to HTTPS sites but does not validate certificates | 09-MARCH-2020 | **7.4 HIGH** | **CVE-2020-8987**  Avast AntiTrack before 1.5.1.172 and AVG Antitrack before 2.0.0.178 proxies traffic to HTTPS sites but does not validate certificates, and thus a man-in-the-middle can host a malicious website using a self-signed certificate. No special action necessary by the victim using AntiTrack with "Allow filtering of HTTPS traffic for tracking detection" enabled. (This is the default configuration.) | https://www.avast.com/hacker-hall-of-fame/en/researcher-david-eade-reports-antitrack-bug-to-avast |
| The Avast AV parsing engine allows virus-detection bypass via a crafted ZIP archive | 28-FEB-2020 | **5.5 MEDIUM** | **CVE-2020-9399**  The Avast AV parsing engine allows virus-detection bypass via a crafted ZIP archive. This affects versions before 12 definitions 200114-0 of Antivirus Pro, Antivirus Pro Plus, and Antivirus for Linux. | Update the latest version. |
| **Application: Joomla** | | | | |
| Multiple vulnerability of Joomla! before 3.9.16 | 16-MARCH-2020 | **8.8**  **HIGH** | **CVE-2020-10238**  **CVE-2020-10239**  **CVE-2020-10240**  **CVE-2020-10241**  **CVE-2020-10242**  Joomla! before 3.9.16 suffer from multiple vulnerability. | Upgrade to version 3.9.16.  https://developer.joomla.org/security-centre/804-20200303-core-incorrect-access-control-in-com-templates  https://developer.joomla.org/security-centre/806-20200305-core-incorrect-access-control-in-com-fields-sql-field  https://developer.joomla.org/security-centre/805-20200304-core-identifier-collisions-in-com-users  https://developer.joomla.org/security-centre/802-20200301-core-csrf-in-com-templates-image-actions  https://developer.joomla.org/security-centre/803-20200302-core-xss-in-protostar-and-beez3 |
| **Application: Nagios** | | | | |
| Nagios NRPE 3.2.1 Filter command injection | 16-MARCH-2020 | **9.8 CRITICAL** | **CVE-2020-6581**  Nagios NRPE 3.2.1 has Insufficient Filtering because, for example, nasty\_metachars interprets \n as the character \ and the character n (not as the \n newline sequence). This can cause command injection. | - |
| Nagios Log Server 2.1.3 cross site request forgery | 16-MARCH-2020 | **8.8**  **HIGH** | **CVE-2020-6585**  Nagios Log Server 2.1.3 has CSRF. | https://assets.nagios.com/downloads/nagios-log-server/CHANGES.TXT  https://www.nagios.com/products/nagios-log-server/ |
| Nagios Log Server 2.1.3 Incorrect Access Control | 16-MARCH-2020 | **6.5 MEDIUM** | **CVE-2020-6584**  Nagios Log Server 2.1.3 has Incorrect Access Control. | https://assets.nagios.com/downloads/nagios-log-server/CHANGES.TXT  https://www.nagios.com/products/nagios-log-server/ |
| **Application: MicroTik**- | | | | |
| MikroTik RouterOS Packet Reboot denial of service | 02-MARCH-2020 | **7.5**  **HIGH** | **CVE-2018-5951**  An issue was discovered in Mikrotik RouterOS. Crafting a packet that has a size of 1 byte and sending it to an IPv6 address of a RouterOS box with IP Protocol 97 will cause RouterOS to reboot imminently. All versions of RouterOS that supports EoIPv6 are vulnerable to this attack. | - |
| **Application: Barracuda** | | | | |
| LDAP Credential Exposure in Barracuda Load Balancer ADC | 12-MARCH-2020 | **6.5 MEDIUM** | **CVE-2019-5648**  Authenticated, administrative access to a Barracuda Load Balancer ADC running unpatched firmware <= v6.4 allows one to edit the LDAP service configuration of the balancer and change the LDAP server to an attacker-controlled system, without having to re-enter LDAP credentials. These steps can be used by any authenticated administrative user to expose the LDAP credentials configured in the LDAP connector over the network. | Users are encouraged to check for available updates to their Barracuda devices. |
| **Application: Fortinet** | | | | |
| FortiManager Cross-Site WebSocket Hijacking (CSWSH) | 15-MARCH-2020 | **8.8**  **HIGH** | **CVE-2019-17654**  An Insufficient Verification of Data Authenticity vulnerability in FortiManager 6.2.1, 6.2.0, 6.0.6 and below may allow an unauthenticated attacker to perform a Cross-Site WebSocket Hijacking (CSWSH) attack. | https://fortiguard.com/psirt/FG-IR-19-191 |
| FortiClient installer DLL Hijacking Vulnerability | 15-MARCH-2020 | **7.8**  **HIGH** | **CVE-2020-9287, CVE-2020-9290**  Multiple unsafe search path vulnerabilities in FortiClient online installers may allow an attacker with control over the directory in which the installers reside to execute arbitrary code on the system via uploading malicious .dll files in that directory. | https://fortiguard.com/psirt/FG-IR-19-060 |
| FortiOS URL redirection attack via the admin password change page | 15-MARCH-2020 | **6.1 MEDIUM** | **CVE-2019-6696**  An improper input validation vulnerability in FortiOS 6.2.1, 6.2.0, 6.0.8 and below until 5.4.0 under admin webUI may allow an attacker to perform an URL redirect attack via a specifically crafted request to the admin initial password change webpage. | https://fortiguard.com/psirt/FG-IR-19-179 |
| **Application: Ansible** | | | | |
| Ansible 2.7.17 and prior, 2.8.9 and prior, and 2.9.6 and prior | 09-MARCH-2020 | **7.8**  **HIGH** | **CVE-2020-1737**  A flaw was found in Ansible 2.7.17 and prior, 2.8.9 and prior, and 2.9.6 and prior when using the Extract-Zip function from the win\_unzip module as the extracted file(s) are not checked if they belong to the destination folder. An attacker could take advantage of this flaw by crafting an archive anywhere in the file system, using a path traversal. This issue is fixed in 2.10. | https://bugzilla.redhat.com/show\_bug.cgi?id=CVE-2020-1737  https://github.com/ansible/ansible/issues/67795  https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FWDK3QUVBULS3Q3PQTGEKUQYPSNOU5M3/  https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QT27K5ZRGDPCH7GT3DRI3LO4IVDVQUB7/  https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/U3IMV3XEIUXL6S4KPLYYM4TVJQ2VNEP2/ |
| Ansible Engine 2.7.17 and prior, 2.8.9 and prior, 2.9.6 and prior | 11-MARCH-2020 | **7.0**  **HIGH** | **CVE-2020-1733**  A race condition flaw was found in Ansible Engine 2.7.17 and prior, 2.8.9 and prior, 2.9.6 and prior when running a playbook with an unprivileged become user. When Ansible needs to run a module with become user, the temporary directory is created in /var/tmp. This directory is created with "umask 77 && mkdir -p <dir>"; this operation does not fail if the directory already exists and is owned by another user. An attacker could take advantage to gain control of the become user as the target directory can be retrieved by iterating '/proc/<pid>/cmdline'. | https://bugzilla.redhat.com/show\_bug.cgi?id=CVE-2020-1733  https://github.com/ansible/ansible/issues/67791 |
| **Application: Google Android** | | | | |
| Google Android | 10-MARCH-2020 | **8.8 HIGH** | **CVE-2020-0032**  In ih264d\_release\_display\_bufs of ih264d\_utils.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-145364230 | https://source.android.com/security/bulletin/2020-03-01 |
| Google Android | 10-MARCH-2020 | **7.8 HIGH** | **CVE-2020-0033**  In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds write due to stale pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144351324 | https://source.android.com/security/bulletin/2020-03-01 |
| Google Android | 10-MARCH-2020 | **7.5 HIGH** | **CVE-2020-0034**  In vp8\_decode\_frame of decodeframe.c, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure if error correction were turned on, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1Android ID: A-62458770 | https://source.android.com/security/bulletin/2020-03-01 |
| Google Android | 10-MARCH-2020 | **7.8 HIGH** | **CVE-2020-0036**  In has Permissions of PermissionMonitor.java, there is a possible access to restricted permissions due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144679405 | https://source.android.com/security/bulletin/2020-03-01 |
| Google Android | 10-MARCH-2020 | **7.5 HIGH** | **CVE-2020-0037, CVE-2020-0038**  In rw\_i93\_sm\_set\_read\_only of rw\_i93.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143106535 | https://source.android.com/security/bulletin/2020-03-01 |
| Google Android | 10-MARCH-2020 | **7.5 HIGH** | **CVE-2020-0039**  In rw\_i93\_sm\_update\_ndef of rw\_i93.cc, there is a possible read of uninitialized data due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143155861 | https://source.android.com/security/bulletin/2020-03-01 |
| **Application: Cisco** | | | | |
| Cisco SD-WAN Solution Buffer Overflow Vulnerability | 19-MARCH-2020 | **7.8 HIGH** | **CVE-2020-3264,**  **CVE-2020-3265, CVE-2020-3266**  A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwclici-cvrQpH9v |
| Cisco Webex Network Recording Player and Cisco Webex Player Arbitrary Code Execution Vulnerabilities | 04-MARCH-2020 | **7.8 HIGH** | **CVE-2020-3127, CVE-2020-3128**  Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200304-webex-player |
| Cisco Remote PHY Device Software Command Injection Vulnerability | 04-MARCH-2020 | **6.7 Medium** | **CVE-2020-3176**  A vulnerability in Cisco Remote PHY Device Software could allow an authenticated, local attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying certain CLI commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise. | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rphy-cmdinject-DpEjeTgF |
| Cisco SD-WAN Solution vManage Stored Cross-Site Scripting Vulnerability | 19-MARCH-2020 | **5.5 Medium** | **CVE-2019-16010, CVE-2019-16012**  A vulnerability in the web UI of the Cisco SD-WAN vManage software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the vManage software. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200318-vmanage-xss |