



SECURITY BULLETIN: May 2021 (TLP-WHITE)

Purpose of Information

This bulletin provides information and a snap understanding of security vulnerabilities that could affect your organization or office. This has been provided to help raise the need to strengthen security areas in preventing and mitigating any threats that could exist in your environment.

Disclaimer:

The sole purpose of this bulletin is to provide public knowledge and awareness in terms of security support on information related to certain security threats. It is not intended to harm or scare a person or entity in whatever way possible. Therefore, under no circumstances will the Ministry of Communications and Information technology be liable for any indirect, incidental, consequential, special, or exemplary damages arising out of or in connection with your access or use of the information and any third-party content and services.

CVE-2018-14718	<i>Remote Code Execution Vulnerability in FasterXML Data Bind</i>
Score: 9.8 CRITICAL	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the slf4j-ext class from polymorphic deserialization. REF 1: Additional Information for CVE-2018-14718
CVE-2021-26583	<i>Remote Code Execution Vulnerability in HP Amplifier Pack</i>
Score: 9.8 CRITICAL	An improper input validation vulnerability in libswmfextractor library prior to SMR APR-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process. REF 2: Additional Information for CVE-2021-26583
CVE-2021-31166	<i>HTTP Protocol Stack Remote Code Execution Vulnerability</i>
Score: 9.8 CRITICAL	Microsoft released patches addressing a critical RCE vulnerability in Windows. This vulnerability allows an unauthenticated attacker to remotely execute code as kernel. This is a wormable vulnerability where an attacker can simply send a malicious crafted packet to the target impacted webserver. REF 3: Additional Information for CVE-2021-31166



CVE-2021-28476	<i>Hyper-V Remote Code Execution Vulnerability</i>
Score: 9.9 CRITICAL	<p>Microsoft released patches addressing a critical RCE in Windows Server that impacts Hyper-V. Though the exploitation of this vulnerability is less likely (according to Microsoft), this should be prioritized for patching since adversaries can abuse this vulnerability and cause Denial of Service (DoS) in the form of a bug check..</p> <p>REF 4: Additional Information for CVE-2021-28476</p>
CVE-2021-31181	<i>SharePoint Remote Code Execution Vulnerability</i>
Score: 8.8 HIGH	<p>This is a remote code execution vulnerability in Microsoft SharePoint server. This server allows unauthenticated users to send specially crafted request to SharePoint server and again unauthorized access as a SharePoint user..</p> <p>REF 5: Additional Information for CVE-2021-31181</p>
CVE-2020-36326	<i>Object Injection Vulnerability in PHPMailer</i>
Score: 9.8 CRITICAL	<p>PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname. NOTE: this is similar to CVE-2018-19296, but arose because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. As an unintended side effect, this fix eliminated the code that blocked addAttachment exploitation.</p> <p>REF 6: Additional Information for CVE-2020-36326</p>
CVE-2020-17510	<i>Authentication Bypass Vulnerability in Apache Shiro</i>
Score: 9.8 CRITICAL	<p>Apache Shiro before 1.7.0, when using Apache Shiro with Spring, a specially crafted HTTP request may cause an authentication bypass.</p> <p>REF 7: Additional Information for CVE-2020-17510</p>
CVE-2020-13942	<i>Code Injection Vulnerability in Apache Unomi</i>
Score: 9.8 CRITICAL	<p>It is possible to inject malicious OGNL or MVEL scripts into the /context.json public endpoint. This was partially fixed in 1.5.1 but a new attack vector was found. In Apache Unomi version 1.5.2 scripts are now completely filtered from the input. It is highly recommended to upgrade to the latest available version of the 1.5.x release to fix this problem.</p> <p>REF 8: Additional Information for CVE-2020-13942</p>



CVE-2020-18020	<i>SQL Injection Vulnerability in PHP SHE Mail System</i>
Score: 9.8 CRITICAL	SQL Injection in PPHP SHE Mail System v1.7 allows remote attackers to execute arbitrary code by injecting SQL commands into the "user phone" parameter of a crafted HTTP request to the "admin.php" component. REF 9: Additional Information for CVE-2020-18020
CVE-2021-21507	<i>Weak Authentication Vulnerability in Dell EMC Firmware</i>
Score: 9.8 CRITICAL	Arbitrary file write vulnerability in vRealize Operations Manager API (CVE-2021-21983) prior to 8.4 may allow an authenticated malicious actor with network access to the vRealize Operations Manager API can write files to arbitrary locations on the underlying photon operating system. REF 10: Additional Information for CVE-2021-21507
CVE-2021-29145	<i>SSRF RCE in Aruba Policy Manager</i>
Score: 9.8 CRITICAL	A remote server-side request forgery (SSRF) remote code execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability. REF 11: Additional Information for CVE-2021-29145
CVE-2021-2248	<i>Remote Code Execution Vulnerability in Oracle Secure Product</i>
Score: 10 CRITICAL	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via SKID to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. REF 12: Additional Information for CVE-2021-2248
CVE-2021-31572	<i>Denial of Service Vulnerability in AWS</i>
Score: 9.8 CRITICAL	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in stream_buffer.c for a stream buffer.



	REF 13: Additional Information for CVE-2021-31572
CVE-2017-3167	<i>Authentication Bypass Vulnerability in Apache httpd</i>
Score: 9.8 CRITICAL	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. REF 14: Additional Information for CVE-2017-3167
CVE-2021-21346	<i>Deserialization Vulnerability in XStream Library</i>
Score: 9.8 CRITICAL	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16. REF 15: Additional Information for CVE-2021-21346
CVE-2020-11975	<i>Privilege Escalation Vulnerability in Apache Unomi</i>
Score: 9.8 CRITICAL	Apache Unomi allows conditions to use OGNL scripting which offers the possibility to call static Java classes from the JDK that could execute code with the permission level of the running Java process. REF 15 : Additional Information for CVE-2020-11975
CVE-2020-11857	<i>Authorization Bypass Vulnerability in Micro Focus Operation Bridge</i>
Score: 9.8 CRITICAL	An Authorization Bypass vulnerability on Micro Focus Operation Bridge Reporter, affecting version 10.40 and earlier. The vulnerability could allow remote attackers to access the OBR host as a non-admin user. REF 16: Additional Information for CVE-2020-11857
CVE-2021-2302	<i>Remote Code Execution in Oracle Fusion</i>
Score: 9.8 CRITICAL	Vulnerability in the Oracle Platform Security for Java product of Oracle Fusion Middleware (component: OPSS). Supported versions that are affected are 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 Platform Security for Java.



	Successful attacks of this vulnerability can result in takeover of Oracle Platform Security for Java. REF 17: Additional Information for CVE-2021-2302
CVE-2021-27135	<i>Denial of Service Vulnerability in xTerm</i>
Score: 9.8 CRITICAL	xterm before Patch #366 allows remote attackers to execute arbitrary code or cause a denial of service (segmentation fault) via a crafted UTF-8 combining character sequence. REF 18: Additional Information for CVE- 2021-27135
CVE-2020-27655	<i>Improper Access Control Vulnerability in Synology Router Manager</i>
Score: 10 CRITICAL	Improper access control vulnerability in Synology Router Manager (SRM) before 1.2.4-8081 allows remote attackers to access restricted resources via inbound QuickConnect traffic. REF 19: Additional Information for CVE 2020-27655
CVE-2019-12725	<i>Remote Code Execution Vulnerability in Zeroshell</i>
Score: 9.8 CRITICAL	Zeroshell 3.9.0 is prone to a remote command execution vulnerability. Specifically, this issue occurs because the web application mishandles a few HTTP parameters. An unauthenticated attacker can exploit this issue by injecting OS commands inside the vulnerable parameters. REF 20: Additional Information for CVE-2019-12725
CVE-2020-11854	<i>Arbitrary Code Execution Vulnerability in Operations Bridge Manager</i>
Score: 10 CRITICAL	Arbitrary code execution vulnerability in Operation bridge Manager, Application Performance Management and Operations Bridge (containerized) vulnerability in Micro Focus products products Operation Bridge Manager, Operation Bridge (containerized) and Application Performance Management. The vulnerability affects: 1.) Operation Bridge Manager versions 2020.05, 2019.11, 2019.05, 2018.11, 2018.05, 10.63,10.62, 10.61, 10.60, 10.12, 10.11, 10.10 and all earlier versions. 2.) Operations Bridge (containerized) 2020.05, 2019.08, 2019.05, 2018.11, 2018.08, 2018.05. 2018.02 and 2017.11. 3.) Application Performance Management versions 9.51, 9.50 and 9.40 with uCMDB 10.33 CUP 3. The vulnerability could allow Arbitrary code execution. REF 21: Additional Information for CVE-2020-11854
CVE-2020-24636	<i>Remote Code Execution Vulnerability in Aruba IAP</i>
Score: 9.8 CRITICAL	A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP) products in version(s): Aruba Instant 6.5.x: 6.5.4.17 and below;



	<p>Aruba Instant 8.3.x: 8.3.0.13 and below; Aruba Instant 8.5.x: 8.5.0.10 and below; Aruba Instant 8.6.x: 8.6.0.5 and below; Aruba Instant 8.7.x: 8.7.0.0 and below. Aruba has released patches for Aruba Instant that address this security vulnerability.</p> <p>REF 22: Additional Information for CVE-2020-24636</p>
--	--

- *The information provided here has been compiled using content from [CVE MITRE](#) and [SANS RISK](#) materials*
- *It is recommended that you keep your software and Systems Patched and Up-to-date with the latest patches.*



REFERENCE AND GUIDES:

- [Understanding Security Traffic Light Protocol\(TLP\)](#)
- [Understanding CVSS Version 3](#)
- [Understanding what is a CVE](#)

CVSS v3 key

This bulletin is using version 3 of the CVSS, note reference below.

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Contact Detail and Additional Support

Beach Road, Level 6,
Tui Atua Tupua Tamasese Efi Building,
Sogi, Private Bag,
Apia, SAMOA
Telephone: +685 26 117

Facsimile: +685 24 671

E-mail: mcit@mcit.gov.ws