TLP: White[1]

Security Bulletin – May 2021

Dear Constituents,

Please find below our monthly roundup of security vulnerabilities for your information and necessary actions to secure your network and assets.

Vulnerabilities with Active Exploits in the Wild

Remote Code Execution Vulnerability in Oracle Secure Product *(CVE-2021-2248)*

Severity: **HIGH**

Description

Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server).

How it works

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

What to do

Be sure to have the appropriate security updates recommended by vendor

Reference

https://www.oracle.com/security-alerts/cpuapr2021.html

1 CERT Tonga adopts the Traffic Light Protocol

Authorization Bypass Vulnerability in Micro Focus Operation Bridge *(CVE-2020-11857, CVE-2020-11854)* Severity: **HIGH**

Description

An Authorization Bypass vulnerability on Micro Focus Operation Bridge Reporter, affecting version 10.40 and earlier.

How it works

The vulnerability could allow remote attackers to access the OBR host as a non-admin user.

What to do

Be sure to have the appropriate security updates recommended by vendor

Reference

https://softwaresupport.softwaregrp.com/doc/KM03710590

Weak Authentication Vulnerability in Dell EMC Firmware *(CVE-2021-21507)*

Severity: **HIGH**

Description

Dell EMC Networking X-Series firmware versions prior to 3.0.1.8 and Dell EMC PowerEdge VRTX Switch Module firmware versions prior to 2.0.0.82 contain a Weak Password Encryption Vulnerability.

How it works

A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable system with privileges of the compromised account.

What to do

Apply the most appropriate security update as recommended by the vendor.

Reference

https://www.vmware.com/security/advisories/VMSA-2021-0004.html

Input Validation Vulnerability in Symantec Security Analytics *(CVE-2021-30642)*

Severity: **HIGH**

Description

An input validation flaw in the Symantec Security Analytics web UI 7.2 prior 7.2.7, 8.1, prior to 8.1.3-NSR3, 8.2, prior to 8.2.1-NSR2 or 8.2.2

How it works

It allows a remote, unauthenticated attacker to execute arbitrary OS commands on the target with elevated privileges.

What to do

Apply the most appropriate security update as recommended by the vendor.

Reference

https://support.f5.com/csp/article/K03009991

SSRF RCE in Aruba Policy Manager and IAP *(CVE-2021-29145, CVE-2020-224636)*

Severity: **HIGH**

Description

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

How it works

A successful exploit allows an attacker to execute arbitrary code on the ClearPass host, leading to total cluster compromise.

What to do

Ensure to apply the appropriate security updates recommended by vendor

Reference

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-009.txt

Remote Code Execution Vulnerability in HP Amplifier Pack *(CVE-2021-26583)*

Severity: **HIGH**

Description

A potential security vulnerability was identified in HPE iLO Amplifier Pack

How it works

The vulnerabilities could be remotely exploited to allow remote code execution.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04129en_us

Object Injection Vulnerability in PHPMailer *(CVE-2020-36326)* Severity: **HIGH**

Description

PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname.

How it works

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.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/3B5WDPGUFNPG4NAZ6G4BZX43BKLAVA5B/

https://github.com/PHPMailer/PHPMailer/commit/e2e07a355ee8ff36aba21d0242c5950c56e4c6f9

Privilege Escalation Vulnerability in Apache Unomi *(CVE-2020-11975)* Severity: **HIGH**

Description

A vulnerability found in Apache Unomi.

How it works

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.

What to do

Apache Unomi users should upgrade to 1.5.1 or later

Reference

http://unomi.apache.org/security/cve-2020-11975.txt

HTTP Protocol Stack Remote Code Execution Vulnerability (*CVE-2021-31166)*

Severity: **HIGH**

Description

Microsoft released patches addressing a critical RCE vulnerability in Windows.

How it works

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

What to do

Be sure to appropriate security updates recommended by Microsoft

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31166

Remote Code Execution in Oracle Fusion *(CVE-2021-2302)* Severity: **HIGH**

Description

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.

How it works

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

What to do

Ensure that you apply the most appropriate updates that is recommended by Vendor

Reference

https://www.oracle.com/security-alerts/cpuapr2021.html

Authentication Bypass Vulnerability in Apache Shiro *(CVE-2020-17510)* Severity: HIGH

Description

Vulnerability found in Apache Shiro.

How it works

Apache Shiro before 1.7.0, when using Apache Shiro with Spring, a specially crafted HTTP request may cause an authentication bypass.

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://lists.apache.org/thread.html/r70b907ccb306e9391145e2b10f56cc6914a245f91720a17a486c020a@%3Cdev.shiro.apache.org%3E

Denial of Service Vulnerability in xTerm *(CVE-2021-27135)* Severity: HIGH

Description

DoS Vulnerability found in xTerm.

How it works

It allows remote attackers to execute arbitrary code or cause a denial of service (segmentation fault) via a crafted UTF-8 combining character sequence.

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://invisible-island.net/xterm/xterm.log.html

Other Vulnerabilities with known Exploits

Improper Access Control Vulnerability in Synology Router Manager *(CVE-2020-27655)* Severity: **MEDIUM**

Description: 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.

Denial of Service Vulnerability in AWS *(CVE-2021-31572)* Severity: **MEDIUM**

Description: The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in stream_buffer.c for a stream buffer.

SharePoint Remote Code Execution Vulnerability (*CVE-2021-31181)* Severity: **MEDIUM**

Description: 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.

Hyper-V Remote Code Execution Vulnerability (*CVE-2021-28476)* Severity: **MEDIUM**

Description: 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.

Privilege Escalation Vulnerability in Plone (*CVE-2021-33509)* Severity: **MEDIUM**

Description: Plone through 5.2.4 allows remote authenticated managers to perform disk I/O via crafted keyword arguments to the ReStructuredText transform in a Python script.

Weak Authentication Vulnerability in MaLion (*CVE-2017-10818)* Severity: **MEDIUM**

Description: MaLion for Windows and Mac versions 3.2.1 to 5.2.1 uses a hardcoded cryptographic key which may allow an attacker to alter the connection settings of Terminal Agent and spoof the Relay Service.

Deserialization Vulnerability in XStream Library (*CVE-2021-21346)* Severity: MEDIUM

Description: 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.

Denial of Service Vulnerability in Hilscher EtherNet (*CVE-2021-20987)* Severity: MEDIUM

Description: A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.

SQL Injection Vulnerability in Codologic (*CVE-2020-13873)* Severity: MEDIUM

Description: A SQL Injection vulnerability in get_topic_info() in sys/CODOF/Forum/Topic.php in Codoforum before 4.9 allows remote attackers (pre-authentication) to bypass the admin page via a leaked password-reset token of the admin. (As an admin, an attacker can upload a PHP shell and execute remote code on the operating system.)

Remote Code Execution Vulnerability in Zeroshell (*CVE-2019-12725)* Severity: MEDIUM

Description: 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.

Authentication Bypass Vulnerability in Apache httpd (*CVE-2021-3167)* Severity: MEDIUM

Description: 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.

Other Vulnerabilities

SQL Injection Vulnerability in PHPSHE Mail System (*CVE-2020-18020)* Severity: **MEDIUM**

Description: SQL Injection in PHPSHE Mall 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.

Compiled with information from SANS' @RISK: The Consensus Security Vulnerability Alerts.

The Severity ratings on the above vulnerabilities are based on the NIST Common Vulnerability Scoring System Calculator (CVSS) version 2.0

For more information please contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga