CERT Tonga

Ministry of Meteorology Energy
Information, Disaster Management,
Environment, Communications and
Climate Change

TLP: White[1]

Security Bulletin – April 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 Injection Vulnerability in D-link devices *(CVE-2021-26810)* Severity: **HIGH**

Description

D-link DIR-816 A2 v1.10 is affected by a remote code injection vulnerability

How it works

. An HTTP request parameter can be used in command string construction in the handler function of the /goform/dir_setWanWifi, which can lead to command injection via shell metacharacters in the statuscheckpppoeuser parameter.

What to do

Be sure to have the appropriate security updates recommended by vendor

Reference

https://www.dlink.com/en/security-bulletin/

Remote Code Execution Vulnerability in VMware vCenter Server Plugin *(CVE-2021-21972, CVE-2021-21973)* Severity: **HIGH**

Description

The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin.

[1] CERT Tonga adopts the Traffic Light Protocol

How it works

A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. This affects VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).

What to do

Be sure to have the appropriate security updates recommended by vendor

Reference

https://www.vmware.com/security/advisories/VMSA-2021-0002.html

Privilege Escalation Vulnerability in VMware vRealize *(CVE-2021-21983)* Severity: **HIGH**

Description

Arbitrary file write vulnerability in vRealize Operations Manager API (CVE-2021-21983) prior to 8.4.

How it works

It allows 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.

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

Remote Code Execution Vulnerability in F5 Big IP system *(CVE-2021-22986)* Severity: **HIGH**

Description

This vulnerability allows for unauthenticated attackers with network access to the iControl REST interface, through the BIG-IP management interface and self IP addresses.

How it works

To execute arbitrary system commands, create or delete files, and disable services. This vulnerability can only be exploited through the control plane and cannot be exploited through the data plane. Exploitation can lead to complete system compromise. The BIG-IP system in Appliance mode is also vulnerable

What to do

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

Reference

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

Authentication Bypass Vulnerability in SAP NetWeaver *(CVE-2020-6287)* Severity: HIGH

Description

SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, does not perform an authentication check.

How it works

This allows an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java system, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system, leading to Missing Authentication Check.

What to do

Ensure to apply the appropriate security updates recommended by vendor

Reference

https://launchpad.support.sap.com/#/notes/2934135

Privilege Escalation Vulnerability in SonicWall Email Security *(CVE-2021-20021)* Severity: HIGH

Description

A vulnerability in the SonicWall Email Security version 10.0.9.x

How it works

It allows an attacker to create an administrative account by sending a crafted HTTP request to the remote host.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0007

Remote Code Execution Vulnerability in MacOS Big Sur *(CVE-2021-1871)* Severity: HIGH

Description

A remote execution vulnerability found in MacOS Big Sur.

How it works

A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://support.apple.com/en-us/HT212146

https://support.apple.com/en-us/HT212147

Remote Code Execution Vulnerability in SAP Commerce *(CVE-2020-27861)* Severity:

HIGH

Description

SAP Commerce, versions - 1808, 1811, 1905, 2005, 2011, Backoffice application allows certain authorized users to create source rules which are translated to drools rule when published to certain modules within the application.

How it works

An attacker with this authorization can inject malicious code in the source rules and perform remote code execution enabling them to compromise the confidentiality, integrity and availability of the application.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649

Authentication Bypass Vulnerability in Pulse Connect Secure *(CVE-2021-22893)* Severity: HIGH

Description

Pulse Connect Secure 9.0R3/9.1R1 and higher is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features of Pulse Connect Secure.

How it works

It allows an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway.

What to do

Be sure to appropriate security updates recommended by the vendor

Reference

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/

Remote Code Execution in Oracle Storage Cloud *(CVE-2021-2256)* Severity: HIGH

Description

Vulnerability in the Oracle Storage Cloud Software Appliance product of Oracle Storage Gateway (component: Management Console).

How it works

The supported version that is affected is Prior to 16.3.1.4.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Storage Cloud Software Appliance. While the vulnerability is in Oracle Storage Cloud Software Appliance, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Storage Cloud Software Appliance

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

Remote Code Execution Vulnerability in Cisco vManage Software *(CVE-2021-1479)* Severity: **HIGH**

Description

Multiple vulnerabilities in Cisco SD-WAN vManage Software

How it works

This could allow an unauthenticated, remote attacker to execute arbitrary code or allow an authenticated, local attacker to gain escalated privileges on an affected system. For more information about these vulnerabilities.

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy

Vulnerability in the Oracle Secure Global Desktop *(CVE-2021-2177)* Severity: **HIGH**

Description

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

How it works

The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP 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

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

Reference

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

Authentication Bypass Vulnerability in Juniper *(CVE-2021-0248)* Severity: **HIGH**

Description

This issue is not applicable to NFX NextGen SoftwareThis issue affects: Juniper Networks Junos OS versions prior to 19.1R1 on NFX Series. No other platforms besides NFX

How it works

On NFX Series devices the use of Hard-coded Credentials in Juniper Networks Junos OS allows an attacker to take over any instance of an NFX deployment. This issue is only exploitable through administrative interfaces.

What to do

Ensure to apply appropriate security updates recommended by the Vendor

Reference

https://kb.juniper.net/JSA11141

Remote Code Execution in Oracle WebLogic Server *(CVE-2021-2135)* Severity: **HIGH**

Description

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Coherence Container).

How it works

Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

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

Authentication Bypass Vulnerability in MicroFocus Device *(CVE-2021-22507)* Severity: HIGH

Description

Authentication bypass vulnerability in Micro Focus Operations Bridge Manager affects versions 2019.05, 2019.11, 2020.05 and 2020.10

How it works

The vulnerability could allow remote attackers to bypass user authentication and get unauthorized access.

What to do

Apply the most appropriate updates recommended by the Vendor

Reference

https://softwaresupport.softwaregrp.com/doc/KM03793283

Arbitrary Code Execution Vulnerability in Cisco Jabber *(CVE-2021-1411)* Severity: HIGH

Description

Multiple vulnerabilities in Cisco Jabber for Windows, Cisco Jabber for MacOS, and Cisco Jabber for mobile platforms.

How it works

This could allow an attacker to execute arbitrary programs on the underlying operating system with elevated privileges, access sensitive information, intercept protected network traffic, or cause a denial of service (DoS) condition.

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-jabber-PWrTATTC

Remote Code Execution Vulnerability in NetGear ProSafe *(CVE-2021-27274)* Severity: **HIGH**

Description

A vulnerability found in NetGear ProSafe

How it works

This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System 1.6.0.26. Authentication is not required to exploit this vulnerability.

What to do

Apply the most appropriate security updates recommended by Vendor

Reference

https://kb.netgear.com/000062688/Security-Advisory-for-Pre-Authentication-Command-Injection-on-NMS300-PSV-2020-0560

Remote Code Execution in VMware View Planner *(CVE-2021-21978)* Severity: **HIGH**

Description

VMware View Planner 4.x prior to 4.6 Security Patch 1 contains a remote code execution vulnerability.

How it works

Improper input validation and lack of authorization leading to arbitrary file upload in logupload web application. An unauthorized attacker with network access to View Planner Harness could upload and execute a specially crafted file leading to remote code execution within the logupload container.

What to do

Apply the most appropriate security updates recommended by Vendor and make sure to update to the latest version.

Reference

https://www.vmware.com/security/advisories/VMSA-2021-0003.html

Other Vulnerabilities with known Exploits

Improper Certificate Authority (CA) certificate validation vulnerability (CVE-2021-3450**)** Severity: **MEDIUM**

Description: The X509_V_FLAG_X509_STRICT flag enables additional security checks of the certificates present in a certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow certificates in the chain that have explicitly encoded elliptic curve parameters was added as an additional strict check. An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a "purpose" has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. All of the named "purpose" values implemented in libcrypto perform this check. Therefore, where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A purpose is set by default in libssl client and server certificate verification routines, but it can be overridden or removed by an application. In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose. OpenSSL versions 1.1.1h and newer are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1h-1.1.1j).

Weak Authentication Vulnerability in GE Mu Firmware (*CVE-2021-27452)* Severity: **MEDIUM**

Description: The software contains a hard-coded password that could allow an attacker to take control of the merging unit using these hard-coded credentials on the MU320E (all firmware versions prior to v04A00.1).

Deserialization Vulnerability in Apache OFBiz (*CVE-2021-26295)* Severity: **MEDIUM**

Description: Apache OFBiz has unsafe deserialization prior to 17.12.06. An unauthenticated attacker can use this vulnerability to successfully take over Apache OFBiz.

Remote Code Execution in Light CMS (*CVE-2021-27112)* Severity: **MEDIUM**

Description: LightCMS v1.3.5 contains a remote code execution vulnerability in /app/Http/Controllers/Admin/NEditorController.php during the downloading of external images. This vulnerability can be exploited remotely and attackers can exploit this vulnerability to deliver malicious code to end users.

Deserialization Vulnerability in XStream Library (*CVE-2021-21345)* 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 who has sufficient rights to execute commands of the host only by manipulating the processed input stream. Users who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types will not be impacted. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.

Arbitrary Code Execution in Android Devices (*CVE-2021-25360)* Severity: **MEDIUM**

Description: An improper input validation vulnerability in libswmfextractor library prior to SMR APR-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process.

SQL Injection Vulnerability in Nagios (*CVE-2021-28925)* Severity: **MEDIUM**

Description: SQL injection vulnerability in Nagios Network Analyzer before 2.4.3 via the o[col] parameter to api/checks/read/.

Privilege Escalation Vulnerability in Netop Vision Pro (*CVE-2021-27193)*

Severity: **MEDIUM**

Description: Incorrect default permissions vulnerability in the API of Netop Vision Pro up to and including 9.7.1 allows a remote unauthenticated attacker to read and write files on the remote machine with system privileges resulting in a privilege escalation

Authentication Bypass Vulnerability in Posimyth WP Plugin (*CVE-2021-24175)*

Severity: **MEDIUM**

Description: The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.7 was being actively exploited to by malicious actors to bypass authentication, allowing unauthenticated users to log in as any user (including admin) by just providing the related username, as well as create accounts with arbitrary roles, such as admin. These issues can be exploited even if registration is disabled, and the Login widget is not active.

Malicious File Upload Vulnerability in WP Library (*CVE-2021-24223)* Severity: **MEDIUM**

Description: The N5 Upload Form WordPress plugin through 1.0 suffers from an arbitrary file upload issue in page where a Form from the plugin is embed, as any file can be uploaded. The uploaded filename might be hard to guess as it's generated with md5(uniqid(rand())), however, in the case of misconfigured servers with Directory listing enabled, accessing it is trivial.

Other Vulnerabilities

SQL Injection Vulnerability in Openclinic (*CVE-2020-27236)* Severity: **MEDIUM**

Description: An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3 in the compnomenclature parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.

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

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services