CERT Tonga

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

TLP: White[1]

Security Bulletin – September 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

Command Injection Vulnerability in D-Link Devices *(CVE-2021-39509)* Severity: HIGH

Description

An issue was discovered in D-Link DIR-816 DIR-816A2_FWv1.10CNB05_R1B011D88210.

How it works

The HTTP request parameter is used in the handler function of /goform/form2userconfig.cgi route, which can construct the user name string to delete the user function. This can lead to command injection through shell metacharacters.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

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

Weak Authentication in TP-Link Devices *(CVE-2020-35575)* Severity: HIGH

Description

A password-disclosure issue in the web interface on certain TP-Link devices. This affects WA901ND devices

[1] CERT Tonga adopts the Traffic Light Protocol

before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices.

How it works

It allows a remote attacker to get full administrative access to the web panel.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://www.tp-link.com/us/security

SQL Injection Vulnerability in Fidelis Network *(CVE-2021-35048)* Severity: **HIGH**

Description

Vulnerability in Fidelis Network and Deception CommandPost. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability

How it works

It enables unauthenticated SQL injection through the web interface. The vulnerability could lead to exposure of authentication tokens in some versions of Fidelis software

What to do

Apply the most appropriate updates as recommended by Venodor

Reference

https://support.fidelissecurity.com/hc/en-us/categories/360001842694-Advisories-News-and-Policies

https://www.securifera.com/blog/2021/06/24/operation-eagle-eye/

Malicious File Upload Vulnerability in Apache OFBiz *(2021-37608)* Severity: **HIGH**

Description

Unrestricted Upload of File with Dangerous Type vulnerability in Apache OFBiz.

How it works

It allows an attacker to execute remote commands

What to do

Upgrade to at least 17.12.07 or apply one of the patches at https://issues.apache.org/jira/browse/OFBIZ-12297

Reference

https://lists.apache.org/thread.html/rfd639ca63c8a80534b65623d9c6068859d17e2dfaaeb00a24e9fec9c@%3Cnotifications.ofbiz.apache.org%3E

Windows WLAN AutoConfig Service Remote Code Execution Vulnerability *(CVE-2021-36965)* Severity: **HIGH**

Description

This vulnerability could allow network adjacent attackers to run their code on affected systems at SYSTEM level.

How it works

This means an attacker could completely take over the target – provided they are on an adjacent network. This would be highly useful in a coffee shop scenario where multiple people are using an unsecured WiFi network. Still, this requires no privileges or user interaction, so don’t let the adjacent aspect of this bug diminish the severity

What to do

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

Reference

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36965

Remote Code Execution Vulnerability in Apache Tapestry *(CVE-2021-27850)* Severity: **HIGH**

Description

A critical unauthenticated remote code execution vulnerability was found all recent versions of Apache Tapestry. The affected versions include 5.4.5, 5.5.0, 5.6.2 and 5.7.0. The vulnerability I have found is a bypass of the fix for CVE-2019-0195. Recap: Before the fix of CVE-2019-0195 it was possible to download arbitrary class files from the classpath by providing a crafted asset file URL.

How it works

An attacker was able to download the file `AppModule.class` by requesting the URL `http://localhost:8080/assets/something/services/AppModule.class` which contains a HMAC secret key. The fix for that bug was a blacklist filter that checks if the URL ends with `.class`, `.properties` or `.xml`. Bypass: Unfortunately, the blacklist solution can simply be bypassed by appending a `/` at the end of the URL: `http://localhost:8080/assets/something/services/AppModule.class/` The slash is stripped after the blacklist check and the file `AppModule.class` is loaded into the response. This class usually contains the HMAC secret key which is used to sign serialized Java objects.

What to do

Ensure to apply the most appropriate updates as recommended by the Vendor.

Reference

https://lists.apache.org/thread.html/r237ff7f286bda31682c254550c1ebf92b0ec61329b32fbeb2d1c8751%40%3Cusers.tapestry.apache.org%3E

Weak Permissions Vulnerability in Cloud Foundry Garden Linux (*CVE-2016-0761)*

Severity: **HIGH**

Description

Cloud Foundry Garden-Linux versions prior to v0.333.0 and Elastic Runtime 1.6.x version prior to 1.6.17 contain a flaw in managing container files during Docker image preparation.

How it works

To exploit the vulnerability, an attacker could be used to delete, corrupt or overwrite host files and directories, including other container filesystems on the host.

What to do

Users of affected versions should apply the following mitigation:

- The Cloud Foundry Foundation recommends that all deployments of Garden-Linux are upgraded to v0.333.0 [1]
- Pivotal recommends that all PCF deployments running Elastic Runtime 1.6.x are upgraded to Elastic Runtime 1.6.17 or higher.

Reference

https://pivotal.io/security/cve-2016-0761

XXE Vulnerability in dom4j library *(CVE-2020-10683)* Severity: **HIGH**

Description

A vulnerability found in domj4 library.

However, there is popular external documentation from OWASP showing how to enable the safe, non-default behavior in any application that uses dom4j.

How it works

dom4j before 2.0.3 and 2.1.x before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks.

What to do

Apply the most appropriate updates as recommended by the Vendor

Reference

https://lists.apache.org/thread.html/r51f3f9801058e47153c0ad9bc6209d57a592fc0e7aefd787760911b8@%3Cdev.velocity.apache.org%3E
https://security.netapp.com/advisory/ntap-20200518-0002/

Other Vulnerabilities with known Exploits

Weak Authentication Vulnerability in Onefuzz Deployment (*CVE-2021-37705)* Severity: **MEDIUM**

Description: OneFuzz is an open source self-hosted Fuzzing-As-A-Service platform. Starting with OneFuzz 2.12.0 or greater, an incomplete authorization check allows an authenticated user from any Azure Active Directory tenant to make authorized API calls to a vulnerable OneFuzz instance. To be vulnerable, a OneFuzz deployment must be both version 2.12.0 or greater and deployed with the non-default --multi_tenant_domain option. This can result in read/write access to private data such as software vulnerability and crash information, security testing tools and proprietary code and symbols. Via authorized API calls, this also enables tampering with existing data and unauthorized code execution on Azure compute resources. This issue is resolved starting in release 2.31.0, via the addition of application-level check of the bearer token's `issuer` against an administrator-configured allowlist. As a workaround users can restrict access to the tenant of a deployed OneFuzz instance < 2.31.0 by redeploying in the default configuration, which omits the `--multi_tenant_domain` option.

XSS Vulnerability in Remark HTML (*CVE-2021-39199)* Severity: **MEDIUM**

Description: remark-html is an open source nodejs library which compiles Markdown to HTML. In affected versions the documentation of remark-html has mentioned that it was safe by default. In practice the default was never safe and had to be opted into. That is, user input was not sanitized. This means arbitrary HTML can be passed through leading to potential XSS attacks. The problem has been patched in 13.0.2 and 14.0.1: `remark-html` is now safe by default, and the implementation matches the documentation. On older affected versions, pass `sanitize: true` if you cannot update.

Buffer Overflow Vulnerability in PowerLogic Devices (*CVE-2021-22714)* Severity: **MEDIUM**

Description: A CWE-119: Improper restriction of operations within the bounds of a memory buffer vulnerability exists in PowerLogic ION7400, PM8000 and ION9000 (All versions prior to V3.0.0), which could cause the meter to reboot or allow for remote code execution.

Cisco APIC Arbitrary File Read and Write Vulnerability (*CVE-2021-1577)* Severity: **MEDIUM**

Description: A vulnerability in an API endpoint of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC) could allow an unauthenticated, remote attacker to read or write arbitrary files on an affected system. This vulnerability is due to improper access control. An attacker could exploit this vulnerability by using a specific API endpoint to upload a file to an affected device. A successful exploit could allow the attacker to read or write arbitrary files on an affected device.

Microsoft MSHTML Remote Code Execution Vulnerability (*CVE-2021-40444)* Severity: **MEDIUM**

Description: MSHTML is the Internet Explorer web browser’s rendering engine, though many Office documents also use this engine. If an adversary were to successfully exploit this vulnerability, they could remotely execute code on the victim machine or gain complete control.

Attackers are using a .DOCX file. Upon opening it, the document loaded the Internet Explorer engine to render a remote web page from the threat actor. Malware is then downloaded by using a specific ActiveX control in the web page. Executing the threat is done using "a trick called 'Cpl File Execution'," referenced in Microsoft's advisory

Arbitrary Code Execution Vulnerability in PG Partition Manager *(CVE-2021-33204)*

Severity: **MEDIUM**

Description: In the pg_partman (aka PG Partition Manager) extension before 4.5.1 for PostgreSQL, arbitrary code execution can be achieved via SECURITY DEFINER functions because an explicit search_path is not set.

Command Injection Vulnerability in BTRbk *(CVE-2021-38173)* Severity: **MEDIUM**

Description: Btrbk before 0.31.2 allows command execution because of the mishandling of remote hosts filtering SSH commands using ssh_filter_btrbk.sh in authorized_keys.

Other Vulnerabilities

Weak Permissions Vulnerability in HashiCorp Vault (*CVE-2021-38553)* Severity: **LOW**

Description HashiCorp Vault and Vault Enterprise 1.4.0 through 1.7.3 initialized an underlying database file associated with the Integrated Storage feature with excessively broad filesystem permissions. Fixed in Vault and Vault Enterprise 1.8.0.

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