TLP: White[1]

Security Bulletin – December 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

Authentication Bypass vulnerability in Dell Networking OS10 (*CVE-2021-36308)* Severity: **HIGH**

Description

Networking OS10, versions prior to October 2021 with Smart Fabric Services enabled, contains an authentication bypass vulnerability.

How it works

A remote unauthenticated attacker could exploit this vulnerability to gain access and perform actions on the affected system.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://www.dell.com/support/kbdoc/en-us/000193076

IP Address privilege escalation vulnerability in the TP-Link TL-WR840N EU v5 router (*CVE-2021-41653)* Severity: **HIGH**

Description

The PING function on the TP-Link TL-WR840N EU v5 router with firmware through TL-WR840N(EU)_V5_171211 is vulnerable to remote code execution via a crafted payload in an IP address input field.

1 CERT Tonga adopts the Traffic Light Protocol

How it works

A remote unauthenticated attacker could exploit this vulnerability to gain access and perform actions on the affected system.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

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

https://k4m1ll0.com/cve-2021-41653.html

Various software products and online services actively exploited due to Log4j vulnerability *(CVE-2021-33271, CVE-2021-33266)* Severity: **HIGH**

Description

Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints.

How it works

An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed

What to do

Ensure that you apply the appropriate updates recommended by the vendor.

Reference

https://logging.apache.org/log4j/2.x/security.html

Stack buffer overflow vulnerability in the D-Link DIR-809 (*CVE-2021-33271, CVE-2021-33266, CVE-2021-33267, CVE- 2021-33268, CVE-2021-33270, CVE-2021-33274)* Severity: **HIGH**

Description

This vulnerability is triggered via a crafted POST request.D-Link.

How it works

DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function sub_80046EB4 in /formSetPortTr.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

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

https://github.com/Lnkvct/IoT-poc/tree/master/D-Link-DIR809/vuln11

Heap overflow in the Qualcomm chipsets (*CVE-2021-1975, CVE-2021-30321)* Severity: **HIGH**

Description

Qualcomm Snapdragon is a line of system-on-a-chip semiconductor products manufactured and marketed by Qualcomm Technologies Inc. for mobile smartphones. Possible heap overflow due to improper length check of domain while parsing the DNS response. This vulnerability is affecting the Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IoT, Snapdragon Industrial IoT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables.

How it works

An attacker can use this in conjunction with log poisoning to gain root rights on a vulnerable access point.

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://www.qualcomm.com/company/product-security/bulletins/november-2021-bulletin

Rowhammer attack variant on modern DRAM devices (*CVE-2021-42114)* Severity: **HIGH**

Description

Dynamic Random-Access Memory (DRAM) is a type of semiconductor memory that is typically used for the data or program code needed by a computer processor to function. These devices are used in personal computers (PCs), workstations, and servers. Modern DRAM devices (PC-DDR4, LPDDR4X) are affected by a vulnerability in their internal Target Row Refresh (TRR) mitigation against Rowhammer attacks.

How it works

Rowhammer is a security flaw in dynamic random-access memory (DRAM) that takes advantage of an unintended and undesirable side effect in which memory cells interact electrically between themselves by leaking their charges, potentially changing the contents of nearby memory rows that were not addressed in the original memory access. Because of the high cell density in the current DRAM, this circumvention of DRAM memory cell isolation can be triggered by specifically constructed memory access patterns that repeatedly activate the same memory rows

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://comsec.ethz.ch/wp-content/files/blacksmith_sp22.pdf
https://comsec.ethz.ch/research/dram/blacksmith/

Local File Inclusion (LFI) vulnerability in the Aerohive/Extreme Networks HiveOS administrative web interface (*CVE-2020-16152)* Severity: **HIGH**

Description

The Aerohive/Extreme Networks HiveOS administrative web interface (NetConfig) is vulnerable to LFI. The old version of PHP used in the interface makes it vulnerable to string truncation attacks.

How it works

An attacker can use this in conjunction with log poisoning to gain root rights on a vulnerable access point.

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://gtacknowledge.extremenetworks.com/articles/Vulnerability_Notice/VN-2020-001

Click-Jacking vulnerability in TIBCO PartnerExpress *(CVE-2021-43048)* Severity: **HIGH**

Description

In TIBCO PartnerExpress versions before 6.2.1, a critical vulnerability was discovered. This problem affects an unidentified function of the Interior Server/Gateway Server component. A privilege escalation vulnerability is created by manipulating an unknown input. CWE-451 is the result of using CWE to declare the problem. Confidentiality, honesty, and availability are all impacted.

How it works

The components listed above contain a vulnerability that theoretically allows an unauthenticated attacker with network access to execute a clickjacking attack on the affected system. A successful attack using this vulnerability does not require human interaction from a person other than the attacker.

What to do

Vendor has released updated versions of the affected systems which address this issue.

Reference

https://www.tibco.com/support/advisories/2021/11/tibco-security-advisory-november-16-2021-tibco-partnerexpress-2021-43048

Buffer overflow vulnerability in CIRCUTOR COMPACT DC-S BASIC (*CVE-2021-26777)* Severity: **HIGH**

Description

Buffer overflow vulnerability in function SetFirewall in index.cgi in CIRCUTOR COMPACT DC-S BASIC smart metering concentrator Firwmare version CIR_CDC_v1.2.17.

How it works

It allows attackers to execute arbitrary code.

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://github.com/Ell0/plc_concentrator_vulns/

Other Vulnerabilities with known Exploits

Unauthenticated remote code execution vulnerability in the Kaseya Unitrends Backup Appliance (*CVE-2021-43033)* Severity: **MEDIUM**

Description: An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. Multiple functions in the bpserverd daemon were vulnerable to arbitrary remote code execution as root. The vulnerability was caused by untrusted input (received by the server) being passed to system calls.

Other Vulnerabilities

Improper authorization vulnerability in 4MOSAn GCB Doctor (*CVE-2021-42338)* Severity: **MEDIUM**

Description: In 4MOSAn GCB Doctor, a major vulnerability was discovered (unknown version). This problem affects an unidentified code
A privilege escalation vulnerability is created by manipulating an unknown input. CWE-285 is the result of using CWE to declare the problem. Confidentiality, honesty, and availability are all impacted.

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.