TLP: White[1]

Security Bulletin – November 2022

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

Vulnerability in Zimbra Collaboration *(CVE-2022-41352)* Severity: **HIGH**

Description

An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0.

How it works

An attacker can upload arbitrary files through amavisd via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public) that can lead to incorrect access to any other user accounts. Zimbra recommends pax over cpio. Also, pax is in the prerequisites of Zimbra on Ubuntu; however, pax is no longer part of a default Red Hat installation after RHEL 6 (or CentOS 6). Once pax is installed, amavisd automatically prefers it over cpio.

What to do

Apply the most appropriate updates as recommended by the Vendor

Reference

https://wiki.zimbra.com/wiki/Security_Center

A vulnerability found in Google Chrome (*CVE-2022-3652)* Severity: **HIGH**

Description

Type confusion in V8 in Google Chrome prior to 107.0.5304.62

1 CERT Tonga adopts the Traffic Light Protocol

How it works

This could allow a remote attacker to potentially exploit heap corruption via a crafted HTML page.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html

Vulnerability found in Apple iOS(*CVE-2022-42795)* Severity: **HIGH**

Description

A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 16, iOS 16, macOS Ventura 13, watchOS 9.

How it works

Processing a maliciously crafted image may lead to arbitrary code execution.

What to do

Make sure to apply the appropriate updates recommended by Apple.

Reference

https://support.apple.com/en-us/HT213446
https://support.apple.com/en-us/HT213486
https://support.apple.com/en-us/HT213487
https://support.apple.com/en-us/HT213488

Multiple vulnerabilities in VMware Workspace ONE Assist (*CVE-2022-31685)* Severity: **HIGH**

Description

VMware Workspace ONE Assist prior to 22.10 contains an Authentication Bypass vulnerability.

How it works

A malicious actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application.

What to do

Make sure to apply the appropriate updates recommended by the Vendor

Reference

https://www.vmware.com/security/advisories/VMSA-2022-0028.html

A remote code execution (RCE) vulnerability in non-default configurations of Fluentd (*CVE-2022-39379)* Severity: **HIGH**

Description

Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on.

How it works

A remote code execution (RCE) vulnerability in non-default configurations of Fluentd allows unauthenticated attackers to execute arbitrary code via specially crafted JSON payloads. Fluentd setups are only affected if the environment variable `FLUENT_OJ_OPTION_MODE` is explicitly set to `object`. Please note: The option FLUENT_OJ_OPTION_MODE was introduced in Fluentd version 1.13.2. Earlier versions of Fluentd are not affected by this vulnerability. This issue was patched in version 1.15.3.

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://github.com/fluent/fluentd/commit/48e5b85dab1b6d4c273090d538fc11b3f2fd8135
https://github.com/fluent/fluentd/security/advisories/GHSA-fppq-mj76-fpj2

Other Vulnerabilities with known Exploits

Vulnerability occurs in Xenstore (CVE-2022-42319) Severity: **MEDIUM**

Description

Xenstore: Guests can cause Xenstore to not free temporary memory When working on a request of a guest, xenstored might need to allocate quite large amounts of memory temporarily. This memory is freed only after the request has been finished completely. A request is regarded to be finished only after the guest has read the response message of the request from the ring page. Thus a guest not reading the response can cause xenstored to not free the temporary memory. This can result in memory shortages causing Denial of Service (DoS) of xenstored.

Password recovery vulnerability in SICK SIM4000 (PPC) (CVE-2022-27582) Severity: **MEDIUM**

Description

Password recovery vulnerability in SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The firmware versions <=1.10.1 allow to optionally disable device configuration over the network interfaces. Please make sure that you apply general security practices when operating the SIM4000. A fix is planned but not yet scheduled.

A vulnerability was found in centreon (CVE-2022-3827) Severity: **MEDIUM**

Description

It has been declared as critical. This vulnerability affects unknown code of the file formContactGroup.php of the component Contact Groups Form. The manipulation of the argument cg_id leads to sql injection. The attack can be initiated remotely. The name of the patch is 293b10628f7d9f83c6c82c78cf637cbe9b907369. It is recommended to apply a patch to fix this issue. VDB-212794 is the identifier assigned to 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 3.0

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.