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

TLP: Clear[1]

Security Bulletin – March 2023

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

Microsoft Word Remote Code Execution Vulnerability *(CVE-2023-21716)* Severity: HIGH

Description

A vulnerability found in Microsoft Word

How it works

The vulnerability is a heap corruption vulnerability found in MS Office Word's RTF parser. When exploited, the vulnerability allows adversaries to execute arbitrary commands with the victim's privileges via malicious RTF files. Even loading the malicious RTF document in the Preview Pane is enough for exploitation, and the victims do not have to open the payload

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://www. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716

Vulnerability in the Oracle WebLogic Server (*CVE-2023-21839)* Severity: HIGH

Description

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and

1 CERT Tonga adopts the Traffic Light Protocol

14.1.1.0.0.

How it works

Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://www.oracle.com/security-alerts/cpujan2023.html

Vulnerability found in SourceCodester *(CVE-2023-0946)* Severity: **HIGH**

Description

A vulnerability has been found in SourceCodester Best POS Management System 1.0 and classified as critical.

How it works

Affected by this vulnerability is an unknown functionality of the file billing/index.php?id=9. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-221593 was assigned to this vulnerability.

What to do

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

Reference

https://vuldb.com/?id.221593

A Vulnerability found in Geo Tools *(CVE-2023-25158)* Severity: **HIGH**

Description

GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore

How it works

SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations.

What to do

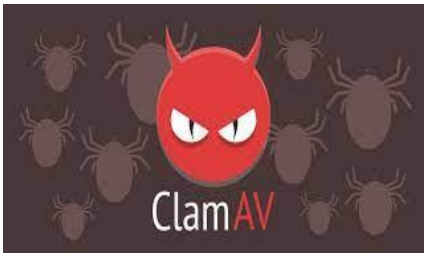
Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue.

Reference

https://github.com/geotools/geotools/security/advisories/GHSA-99c3-qc2q-p94m

A Vulnerability found in ClamAV scanning (*CVE-2023-20032)* Severity: **HIGH**

Description



A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code.

How it works

This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition.

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy

A Vulnerability found in IBM product (*CVE-2023-27290)* Severity: **HIGH**

Description

Docker based datastores for IBM Instana (IBM Observability with Instana 239-0 through 239-2, 241-0 through 241-2, and 243-0) do not currently require authentication.

How it works

Due to this, an attacker within the network could access the datastores with read/write access

What to do

Apply the most appropriate updates recommended by vendor.

Reference

https://www.ibm.com/support/pages/node/6959969

A vulnerability was found in WebKit *(CVE-2019-8720)* Severity: HIGH

Description

A vulnerability was found in WebKit.

How it works

The flaw is triggered when processing maliciously crafted web content that may lead to arbitrary code execution. Improved memory handling addresses the multiple memory corruption issues.

What to do

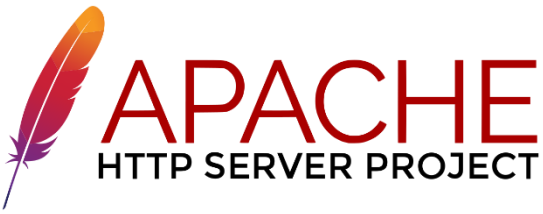
Apply the appropriate update for your system.

Reference

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21568

A Vulnerability identified in COMOS *(CVE-2023-24482)* Severity: HIGH

Description



A mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.

How it works

Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.

What to do

Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

Reference

https://httpd.apache.org/security/vulnerabilities_24.html
https://lists.debian.org/debian-lts-announce/2023/04/msg00028.html

A Vulnerability found in Fortinet (*CVE-2022-41328)* Severity: **HIGH**

Description

A Vulnerability found in Fortinet.

How it works

An improper limitation of a pathname to a restricted directory vulnerability ('path traversal') [CWE-22] in Fortinet FortiOS version 7.2.0 through 7.2.3, 7.0.0 through 7.0.9 and before 6.4.11 allows a privileged attacker to read and write files on the underlying Linux system via crafted CLI commands

What to do

Apply the appropriate updates recommended by the Vendor.

Reference

https://fortiguard.com/psirt/FG-IR-22-369

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

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.