TLP: Clear[1]

Security Bulletin – February 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

Vulnerability in Zoho Manage Engine *(CVE-2022-47966)* Severity: HIGH

Description

Multiple Zoho ManageEngine on-premises products, such as ServiceDesk Plus through 14003 etc.

How it works

This allows remote code execution due to use of Apache xmlsec (aka XML Security for Java) 1.4.1, because the xmlsec XSLT features, by design in that version, make the application responsible for certain security protections, and the ManageEngine applications did not provide those protections.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

Buffer overflow vulnerability in FortiOS (*CVE-2022-42475)* Severity: HIGH

Description

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.10, 6.2.0 through 6.2.11, 6.0.15 and earlier.

1 CERT Tonga adopts the Traffic Light Protocol

How it works

This may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://fortiguard.com/psirt/FG-IR-22-398

Vulnerability found in TerraMaster(*CVE-2022-24990)* Severity: **HIGH**

Description

A flaw was found in TerraMaster NAS 4.2.29 and earlier version.

How it works

This allows remote attackers to discover the administrative password by sending "User-Agent: TNAS" to module/api.php?mobile/webNasIPS and then reading the PWD field in the response.

What to do

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

Reference

https://forum.terra-master.com/en/viewforum.php?f=28
https://octagon.net/blog/2022/03/07/cve-2022-24990-terrmaster-tos-unauthenticated-remote-command-execution-via-php-object-instantiation/

Microsoft SQL Server Remote Code Execution Vulnerability (*CVE-2023-21529)*

Severity: **HIGH**

Description

Microsoft SQL Server Remote Code Execution Vulnerability

How it works

The attacker exploits the vulnerability by accessing the target system locally (e.g., keyboard, console), or remotely (e.g., SSH); or the attacker relies on User Interaction by another person to perform actions required to exploit the vulnerability (e.g., tricking a legitimate user into opening a malicious document)

What to do

A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available.

Reference

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529

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

Description

Microsoft Word Remote Code Execution Vulnerability

How it works

A vulnerability within Microsoft Office's wwlib allows attackers to achieve remote code execution with the privileges of the victim that opens a malicious RTF document. The attacker could deliver this file as an email attachment (or other means).

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

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

A Vulnerability found in IBM product (*CVE-2022-47986)* Severity: HIGH

Description

A vulnerability found in IBM Asper Faspex

How it works

IBM Aspera Faspex 4.4.1 could allow a remote attacker to execute arbitrary code on the system, caused by a YAML deserialization flaw. By sending a specially crafted obsolete API call, an attacker could exploit this vulnerability to execute arbitrary code on the system. The obsolete API call was removed in Faspex 4.4.2 PL2. IBM X-Force ID: 243512

What to do

Apply the appropriate update for your system.

Reference

https://www.ibm.com/support/pages/node/6952319?_ga=2.262801804.1067073978.1678847316-574210541.1664923581

Microsoft SQL Server Integration Service (VS extension) Remote Code Execution Vulnerability *(CVE-2023-21568)* Severity: **HIGH**

Description

A vulnerability has been identified in Microsoft SQL Server Integration Service.

How it works

The vulnerability allows a remote attacker to perform a denial of service (DoS) attack. The vulnerability exists due to insufficient validation of user-supplied input within the Microsoft SQL Server Integration Service (VS extension). A remote attacker can trick the victim to open a specially crafted file and execute arbitrary code on the server.

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 vulnerability has been identified in COMOS V10.2 (All versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions < V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions < V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25).

How it works

Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition.

What to do

Apply the appropriate update for your system.

Reference

https://cert-portal.siemens.com/productcert/pdf/ssa-693110.pdf

A Vulnerability found in DOMPDF (*CVE-2022-47986)* Severity: **HIGH**

Description

Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute.

How it works

An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

What to do

Apply the appropriate update for your system.

Reference

https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa

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.