TLP: White[1]

Security Bulletin – October 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

Remote code execution vulnerability in Apache Common Text (CVE-2022-42889) Severity: **HIGH**

Description

An arbitrary code execution vulnerability was reported in the Apache Common Text library (Text4Shell).

How it works

The vulnerability exists when StringSubstitutor is used with the default interpolators object. The vulnerability could be exploited to trigger an arbitrary code execution when untrusted input is passed on to certain StringSubstitutor methods.

What to do

Apply the most appropriate updates as recommended by the Vendor

Reference

https://lists.apache.org/thread/n2bd4vdsgkqh2tm14l1wyc3jyol7s1om

Remote code execution vulnerability in Sophos Firewall (*CVE-2022-3236)* Severity: **HIGH**

Description

Critical severity actively exploited remote code execution vulnerability in Sophos firewall products.

How it works

1 CERT Tonga adopts the Traffic Light Protocol

This code injection vulnerability can allow an attacker to execute commands remotely on the affected systems. CISA has also added this vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce

Sandbox bypass vulnerability in vm2 (*CVE-2022-36067)* Severity: **HIGH**

Description

vm2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules.

How it works

In versions prior to version 3.9.11, a threat actor can bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. This vulnerability was patched in the release of version 3.9.11 of vm2. There are no known workarounds

What to do

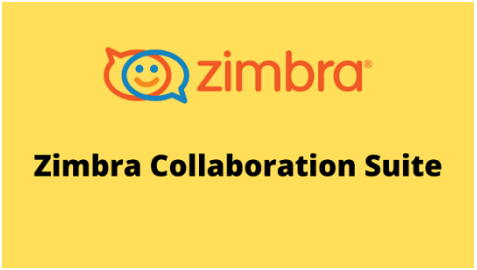
Make sure to apply the appropriate updates recommended by Vendor

Reference

https://github.com/patriksimek/vm2/security/advisories/GHSA-mrgp-mrhc-5jrq
https://www.oxeye.io/blog/vm2-sandbreak-vulnerability-cve-2022-36067

Remote code execution vulnerability in Zimbra Collaboration Suite (*CVE-2022-41352)*

Severity: **HIGH**



Description

Zimbra Collaboration Suite (ZCS) has an actively exploited remote code execution vulnerability.

How it works

This remote code execution vulnerability results from the unsafe use of the cpio utility. Especially from the use of the vulnerable cpio application to scan inbound emails by Zimbra's antivirus engine (Amavis).

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

Microsoft Exchange Server multiple vulnerabilities (*CVE-2022-41082, CVE-2022-41040)*

Severity: **HIGH**

Description

The first flaw (CVE-2022-41040) is a Server-Side Request Forgery (SSRF) vulnerability. The second flaw (CVE-2022-41082) allows remote code execution (RCE) when PowerShell is accessible to the attacker. The customers should know that authenticated access to the vulnerable Exchange Server is necessary to successfully exploit either of the two vulnerabilities

How it works

An attacker could trick a user to open a crafted PDF file, triggering the heap buffer overflow that could lead to memory corruption or a denial of service.

What to do

Apply the most appropriate updates as recommended by the Vendor

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082

Other Vulnerabilities with known Exploits

Heap-based overflow vulnerability in AP4_Atom::TypeFromString (CVE-2022-41429)

Severity: **MEDIUM**

Description

This issue affects the function AP4_Atom::TypeFromString of the component mp4tag. Manipulation with an unknown input may lead to a memory corruption vulnerability.

Heap-based overflow vulnerability in Axiomatic Bento4 mp4mux ReadBit function (CVE-2022-41430) Severity: **MEDIUM**

Description

The flaw affects the function AP4_BitReader::ReadBit of the component mp4mux. Manipulation with an unknown input may lead to a memory corruption 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 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