UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00235

DECEMBER - PATCH TUESDAY

DATE ISSUED: 21st December 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

67 updates are available for Microsoft's Patch Tuesday update in December, with the most severe allowing for Remote Code Execution (RCE) with access as an authenticated user. Depending on that user's privilege, an attacker could install programs as well as view modify or destroy data or even create new accounts with full access. Those with administration level accounts will be more severely impacted than users with fewer rights. Being tracked as CVE-2021-43890, this vulnerability is under known attack in the wild and is being exploited to distribute Emotet, Trickbot and Bazaloader – malware known as loaders which download further malware once installed.

BREAKDOWN

Microsoft Windows:

- 67 updates in total
- 7 rated CRITICAL
- 60 rated IMPORTANT
- In summary: 6 zero days, 21 elevation of privilege, 26 RCE, 10 information disclosure, 3 Denial of Service, 7 Spoofing.

Other vendor releases:

- Google Chrome
- Mozilla
- Apple
- Android
- SAP

REMEDIATION STEPS

- Back up all critical data before performing updates.
- Install latest security updates and patches – For a full list see the resources listed below.

REFERENCES & RESOURCES

Microsoft	https://msrc.microsoft.com/update-guide https://msrc.microsoft.com/update-guide/releaseNote/2021-Dec
Bleeping Computer	https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2021-patch-tuesday-fixes-6-zero-days-67-flaws/
Krebs on Security	https://krebsonsecurity.com/2021/12/microsoft-patch-tuesday-december-2021-edition/
Android	https://source.android.com/security/bulletin/2021-12-01
Apple	https://support.apple.com/en-us/HT201222
SAP	https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+December+2021
VMWare – Log4j	https://www.vmware.com/security/advisories/VMSA-2021-0028.html