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

CYBER GUIDANCE ISSUE 00195

MICROSOFT MSHTML VULNERABILITY EXPLOIT

DATE ISSUED: 13th September 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A vulnerability in Microsoft MSHTML is under active exploitation in the wild and has the potential to allow for Remote Code Execution (RCE). By crafting special Microsoft Office documents, attackers are targeting users in an attempt to gain access to their network and systems.

BREAKDOWN

Microsoft Office documents are becoming an increasingly popular vector for attackers and in this instance, they are seen to be using malicious ActiveX controls used by Microsoft Office documents that hosts the browser rendering engine. Using phishing and social engineering techniques, the malicious actors will attempt to convince a user to open the malicious documents. MSHTML is a component used by numerous Windows applications, including Internet Explorer, in the background and this vulnerability is expected to have a very long shelf-life. The vulnerability is being tracked under MITRE CVE-2021-40444. Systems affected include Windows Server 2022, 2019, 2016, 2012, 2012 R2, 2008, 2008R2, &2004 as well as Windows RT 8.1, 8.1, & Windows 10.

REMEDIATION STEPS

- Ensure users have access rights to services and systems based on their needs in line with the principles of least privilege and need to know access.
- Use simulated phishing training campaigns to assess your users and as a training tool to help users identify malicious emails and know how to report them within your organisation.
- Educate users on the dangers of social engineering and consequences of phishing attacks.
- Ensure Microsoft Defender is up to date and enabled to provide detection and protection.
- Apply the latest security patches and review mitigations and workarounds provided in Microsoft resource below.

REFERENCES & RESOURCES

Microsoft https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
ZDNet https://www.zdnet.com/article/microsoft-cisa-urge-use-of-mitigations-and-workarounds-for-office-document-vulnerability
CIS Advisory