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

CYBER GUIDANCE ISSUE 00201

MICROSOFT MSHTML EXPLOITED BY RYUK GANG

DATE ISSUED: 20th September 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A Ryuk Ransomware gang has seized the opportunity to cash in on organisations who have yet to patch the MSHTML (Cyber Guidance Issue 0199) and seize control of their systems. CVE-2021-40444.

BREAKDOWN

Exploiting the Remote Code Execution (RCE) bug that allows the crafting and sending of malicious Office Documents through email, an attack group is deploying Ryuk ransomware to victims. Microsoft and RiskIQ released two reports to provide insights as to who is exploiting the flaw and recent campaigns. The vulnerability has been addressed in the latest round of security patches issued by Microsoft for September 2021 (Cyber Guidance .

REMEDIATION STEPS

- Apply latest security patches and updates.
- Avoid accessing any Microsoft Office documents you are not expecting to receive.
- Use MFA where possible and disable unnecessary Internet facing services.
- Use good password practices to secure against multiple account compromise.
- 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 consequence of phishing attacks
- Ensure Microsoft Defender is up to date and enabled to provide detection and protection.
- Download Unisphere's free Ransomware Defence Strategy Checklist to check how secure you are and start hardening your environment.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/microsoft-mshtml-ryuk-ransomware/174780/