Marymount University
ITS Department

Memo

To: Ito Sorto, Senior Support Analyst

From: Richard Flores, Student Intern

cc: Dr. Alex Mbaziira, Associate Professor

Date: September 11, 2024

Re: Recent Vulnerabilities Leveraged in Ransomware Attacks by RansomHub

---

This memo serves to bring your attention to two recently executed vulnerabilities that could potentially affect the university's systems.

On August 29, 2024, the FBI, CISA and other agencies released a #StopRansomware advisory warning of recent activities by RansomHub, a ransomware-as-a-service group formed in February 2024. To date, they have encrypted and stolen data from at least 210 victims across both the government and private sectors. This ransomware group often uses a "double-extortion model," meaning not only does the victim have to pay the ransom to get access back to their data, but if payment is not made the ransomware group publishes the data to the internet.

The group uses a combination of email phishing, password spraying, and exploitation of unpatched vulnerabilities to gain access. Tools such as AngryIPScanner, CrackMapExec, Nmap, and PowerShell are used by the group scan for vulnerabilities. Vulnerabilities are then exploited using Cobalt Strike, Metasploit, Kerberoast, and Sliver. Once breached, the group uses lateral movement and privilege escalation to both re-enable default accounts and create new accounts, along with installation of remote desktop software such as PsExec, Anydesk, Connectwise, and N-Able to gain and maintain persistence into the systems. They also use Mimikatz to gather credentials from compromised systems memory which may assist in breaching more systems. Tools such as BITSAdmin, PuTTY, Rclone, and WinSCP are used for data exfiltration of victim data. When ready, the ransomware group will use an elliptic curve encryption algorithm called Curve 25519 to encrypt the victim systems, including stopping many running services to make sure as much data as possible is encrypted. The encryption is started when an unsuspecting victim runs an executable file, often named something innocuous such as "windows.exe" or "update.exe," left on the device's desktop or downloads directories.

One vulnerability leveraged by RansomHub includes CVE-2023-27997. The vulnerability allows buffer overflow attacks on Fortinet products using FortiOS, FortiOS-6K7K, or FortiProxy. It is rated 9.2 on the CVSSv3.1 scale, a CRITICAL vulnerability. The vulnerability can be patched with an update, except on products unable to update past version 1.2, where it remains and cannot be resolved. Leveraging this vulnerability allows the attacker to execute arbitrary remote code.

Another vulnerability used by the group is CVE-2023-46604. This vulnerability affects two Apache products: Apache ActiveMQ and the Apache ActiveMQ Legacy OpenWire Module. This is a CRITICAL vulnerability, rated as a 10.0 on the CVSSv3.1 scale. It allows the attacker to execute arbitrary code by taking advantage of the vulnerability within the Java based OpenWire protocol. Patching of systems will resolve this issue.

Halliburton, an energy company that primarily deals in the oil sector, was one of RansomHubs most recent targets, becoming a victim of an attack by the group on August 21, 2024. As this is such a recent attack, full impacts are not yet known, but Halliburton was forced to take some of their systems offline to mitigate permanent impacts to their systems, causing their customers to be unable to receive invoices or pay their bills. The ransom group was able to get an encryptor executable onto their systems named “maintenance.exe” that initiated the ransom attack.

Threat and risk mitigation: CISA recommends the following actions to mitigate threats from this ransomware group:

1. Implement a recovery plan and maintain offsite, encrypted backups of systems and data
2. Require accounts to use passwords the follow security best practices
3. Keep operating systems, software, and firmware patched with most recent updates
4. Use phishing-resistant MFA (non-SMS based)
5. Implement network segmentation
6. Monitor and respond to suspicious activity on the network
7. Install and update anti-virus/anti-malware software on all nodes
8. Monitor, audit, and disable unused or unauthorized accounts
9. Disable unused ports
10. Implement email security policies, including banners for external emails and disable links
11. Disable macros, command-line, and scripting permissions on standard accounts

Should our systems be affected by these vulnerabilities, CISA recommends the following actions for incident response:

1. Take affected systems offline and quarantine
2. Reimage affected systems
3. Discontinue use and replace any compromised accounts
4. Collect and review evidence, indicators of compromise, and record and recent unusual or suspicious activity
5. Report the incident to CISA at report@cisa.gov or 888-282-0870.

Sources:

"Fogerlog". *Halliburton Falls Victim To RansomHub Ransomware*. Canary Wharf, London, UK. 3 September 2024. Accessed 11 September 2024. https://phishingtackle.com/articles/halliburton-falls-victim-to-ransomhub-ransomware.

CISA. *Cybersecurity Advisory #StopRansomware: RansomHub Ransomware*. Washington, D.C. 29 August 2024. Accessed 11 September 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a.

Lakshmanan, Ravie. *RansomHub Ransomware Group Targets 210 Victims Across Critical Sectors*. New York, NY. 2 September 2024. Accessed 11 September 2024. https://thehackernews.com/2024/09/ransomhub-ransomware-group-targets-210.html.

MITRE Corporation. *CVE-2023-27997*. McLean, VA. 13 June 2023. Accessed 11 September 2024. https://www.cve.org/CVERecord?id=CVE-2023-27997.

MITRE Corporation. *CVE-2023-46604*. McLean, VA. 27 October 2023. Accessed 11 September 2024. https://www.cve.org/CVERecord?id=CVE-2023-46604.