AL2024_15 Veeam Backup & Replication Software Security Flaw Exploited by New Ransomware Group: EstateRansomware (15th July 2024)

Description

A newly identified ransomware group, EstateRansomware, has exploited a patched flaw in Veeam Backup & Replication software to carry out sophisticated cyberattacks. In early April 2024, researchers discovered this group's modus operandi involves leveraging CVE-2023-27532, a vulnerability with a CVSS score of 7.5. The attacks, which could have a significant impact, are further facilitated by using a defunct account on a Fortinet FortiGate firewall SSL VPN appliance, allowing initial access to the target environment.

Attack Details

Initial Access and Lateral Movement:

The initial access was achieved through a Fortinet FortiGate firewall using the SSL VPN service. EstateRansomware leveraged an inactive account, 'Acc1,' to perform brute-force attempts, which were recorded in April 2024. The successful VPN login from a remote IP address using 'Acc1' enabled the threat actors to shift laterally to the failover server.

Backdoor Installation:

To maintain access, the attackers established RDP connections between the firewall and the failover server and installed a permanent backdoor named "svchost.exe." This backdoor runs daily as part of a scheduled job, establishing an HTTP connection with a command-and-control (C2) server to execute commands issued by the attackers.

Exploitation of Veeam Backup & Replication Vulnerability:

Using the flaw CVE-2023-27532, the threat actors enabled xp_cmdshell on the backup server and created a rogue user account named "VeeamBkp." This account facilitated network discovery, enumeration, and credential harvesting using tools like NetScan, AdFind, and NitSoft. The exploitation likely involved attacking the

backup server's vulnerable Veeam installation from the VeeamHax folder on the file server.

Disabling Security Measures:

The attackers used DC.exe (Defender Control) to permanently disable Windows Defender and deployed and executed malware with the PsExec.exe process.

Double Extortion Strategy:

EstateRansomware employs a twofold extortion strategy involving data exfiltration before file encryption. They use custom tools like Exmatter, Exbyte, and StealBit to transfer sensitive data to their controlled infrastructure. The threat actors aim for prolonged access to the victim networks, blending in and escalating their privileges to identify valuable data for theft.

Indicators of Compromise (IOCs)

- VPN brute-force attempts using a dormant account ("Acc1").
- Successful VPN login from remote IP addresses: 149.28.106.252, 45.76.232.205 and 77.238.245.11.
- Establishment of RDP connections from the firewall to the failover server.
- Presence of persistent backdoor "svchost.exe" executed via a scheduled task.
- Creation of rogue user account "VeeamBkp".
- Use of tools: NetScan, AdFind, NitSoft, DC.exe (Defender Control), PsExec.exe.

File Hashes:

- **MD5:** 58008524a6473bdf86c1040a9a9e39c3
- **SHA-256:** 1ef6c1a4dfdc39b63bfe650ca81ab89510de6c0d3d7c608ac5be80033e55932
- **SHA-1**: cb704d2e8df80fd3500a5b817966dc262d80ddb8

Recommendations

1. **Block Threat Indicators:**
   Block all identified threat indicators (IP addresses and file hashes) at your respective controls.
2. **Search for IoCs:**

Utilize your security controls to search for indicators of compromise within your environment.

3. **Regular Security Assessments:**
   Conduct regular security assessments and penetration testing to identify and mitigate vulnerabilities in critical infrastructure and government systems.
4. **Advanced Threat Detection Tools:**
   Advanced threat detection tools, such as Endpoint Detection and Response (EDR) and Network Traffic Analysis (NTA), can be deployed to monitor suspicious activities and anomalies.
5. **Timely Patching and Updates:**
   Ensure timely patching and updating of all software and systems to close known security gaps.
6. **Multi-Factor Authentication (MFA):**
   Use multi-factor authentication and strong password policies to protect user accounts from unauthorized access.
7. **Network Segmentation:**
   Segment networks to limit lateral movement within the organization in case of a breach.
8. **Incident Response Plan:**
   Develop and maintain an incident response plan that includes procedures for ransomware attacks and data breaches.
9. **Employee Training:**
   Train employees on cybersecurity best practices and phishing awareness to reduce the risk of social engineering attacks.
10. **Regular Data Backups:**
    Regularly back up critical data and ensure backups are stored securely and are not accessible from the primary network.
11. **Data Encryption:**
    Implement encryption for sensitive data at rest and in transit to protect against theft.

Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (2024, July 10). New ransomware group exploiting VEEAM backup software vulnerability. Retrieved from Hackers news.

https://thehackernews.com/2024/07/new-ransomware-group-exploiting-veeam.html

- Rewterz. (2024, July 11). VEEAM Backup software vulnerability actively exploited by new ransomware group – active IOCs - Rewterz. Retrieved from *Rewterz - Revolutionizing Cybersecurity*. https://www.rewterz.com/threat-advisory/veeam-backup-software-vulnerability-actively-exploited-by-new-ransomware-group-active-iocs