Active Exploitation of Veeam RCE Vulnerability - CVE-2024-40711

Overview

A critical remote code execution (RCE) vulnerability in Veeam Backup & Replication, tracked as CVE-2024-40711 (CVSS 9.8), is being actively exploited by attackers to deploy ransomware. The attackers are leveraging this vulnerability, in conjunction with compromised credentials, to gain unauthorized access and execute ransomware.

CVE-2024-40711 is an unauthenticated RCE vulnerability that allows attackers to remotely execute arbitrary code without authentication, providing them with control over the targeted system.

Affected Products:

- Veeam Backup & Replication (versions 12.1.2.172 and earlier)
- Veeam ONE
- Veeam Service Provider Console
- Veeam Agent for Linux
- Veeam Backup for Nutanix AHV
- Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization

Sophos detected a surge in attacks utilizing this vulnerability. In multiple instances, attackers used the vulnerability to create privileged user accounts and deploy ransomware. Threat actors include:

- **Fog Ransomware (attack)**
  - A successful deployment on an unprotected Hyper-V server, with data exfiltration using the rclone tool.
- **Akira Ransomware (attempts)**

Exploitation of CVE-2024-40711 typically begins with compromised VPN gateways lacking multifactor authentication (MFA) or running outdated software. Attackers then exploit the Veeam vulnerability by manipulating the Veeam.Backup.MountService.exe process, triggering the RCE on port 8000. Aspire recommends patching immediately.

Aspire Protects

- **Apply Patches**: Apply the latest Veeam update (VBR version 12.2.0.334) that addresses CVE-2024-40711. See Veeam's advisory for patch guidance and details regarding other vulnerabilities.
- Ensure multifactor authentication is enforced on all VPN gateways and remote access services.
- Replace or update any VPNs running unsupported versions to reduce entry points.

IoCs

- **Local Account Creation** - "point" account added to local Administrators and Remote Desktop groups.
- **Exploitation Activity** - Unauthorized use of the Veeam.Backup.MountService.exe and net.exe.
- **Fog Ransomware**
  - **IPv4**
    - 85[.]209[.]11[.]227
    - 85[.]209[.]11[.]254
    - 85[.]209[.]11[.]27
- **Akira Ransomware**
  - **MD5**
    - 08bd63480cd313d2e219448ac28f72cd
    - 4aecef9ddc8d07b82a6902b27f051f34
    - a1f4931992bf05e9bff4b173c15cab15
    - ab9e577334aeb060ac402598098e13b9
    - e57340a208ac9d95a1f015a5d6d98b94
    - e8139b0bc60a930586cf3af6fa5ea573
  - SHA1
    - 0481b7dd0e472eef2819af861961950c6e54b9a0
    - 4549f715bfeab0477c816dc7629b3d50963c4d23
    - 8ad1b4ed98794e8f0a9a9d6fc161697974099d91
  - SHA256
    - 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d
    - 988776358d0e45a4907dc1f4906a916f1b3595a31fa44d8e04e563a32557eb42
    - b5e757f5e240af04057131ab6868a7716c46fa5abf697f2927199d1b84706c23

TTPs to Watch

Initial Access (TA0001)

- Exploitation of Public-Facing Application (T1190) – Attackers exploit the Veeam RCE vulnerability (CVE-2024-40711) to gain unauthorized access to the system.
- Valid Accounts (T1078) – Attackers use compromised credentials, often from VPN gateways without MFA, to gain initial access.

Privilege Escalation (TA0004)

- Create or Modify System Process (T1543.003**)** – Attackers create a local account ("point") and assign it to the Administrators and Remote Desktop groups, allowing privileged access.
- Exploitation for Privilege Escalation (T1068) – Attackers exploit the Veeam vulnerability to escalate privileges by executing unauthorized code.

Defense Evasion (TA0005)

- Obfuscated Files or Information (T1027) – Attackers use tools like rclone to exfiltrate data while bypassing detection.
- Impair Defenses (T1562) – Attackers disable or evade endpoint protections to deploy ransomware.

Lateral Movement (TA0008)

- Remote Services - Remote Desktop Protocol (T1021.001) – Attackers use Remote Desktop after creating a local account with administrative privileges.

Impact (TA0040)

- Data Encrypted for Impact (T1486) – Attackers deploy ransomware (Fog and Akira) to encrypt critical systems.
- Data Destruction (T1485) – In addition to ransomware deployment, attackers may delete backups or destroy data to maximize the impact.

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Security Services**
  - Aspire Managed Security Services provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates “noise” and make sense of what really matters.
  - Our managed security portfolio includes:
    - Managed Firewall
    - Managed IDS/IPS
    - Security event monitoring & incident management
    - Managed Cisco ISE (Identity Services Engine)
    - Endpoint Protection

Supporting Documentation

KB4649: Veeam Security Bulletin (September 2024)

Threat Brief: Understanding Akira Ransomware – LevelBlue – Open Threat Exchange (alienvault.com)

NHS England Warns of Critical Veeam Vulnerability Under Active Exploit - Infosecurity Magazine (infosecurity-magazine.com)