Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Veeam Backup & Replication RCE Flaw Opens Door for Ransomware Attacks

Date of Publication	Admiralty Code	TA Number
October 11, 2024	A1	TA2024391

Summary

First Seen: September 4, 2024
Affected Product: Veeam Backup & Replication
Malware: Akira ransomware, Fog ransomware
Impact: CVE-2024-40711 is a critical RCE vulnerability in Veeam Backup & Replication. This vulnerability allows unauthenticated attackers to execute arbitrary code remotely, potentially granting them full control over affected systems. Recent ransomware attacks, such as Fog and Akira, leveraged this flaw, often using compromised VPNs lacking multifactor authentication. Organizations should patch VBR systems, update VPNs, and enforce MFA to prevent unauthorized access.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-40711	Veeam Backup & Replication Remote Code Execution Vulnerability	Veeam Backup & Replication	✗	✗	✓
CVE-2024-40713	Veeam Backup & Replication Multi-Factor Authentication Bypass Vulnerability	Veeam Backup & Replication	✗	✗	✓
CVE-2024-40710	Veeam Backup & Replication Remote Code Execution Vulnerability	Veeam Backup & Replication	✗	✗	✓
CVE-2024-39718	Veeam Backup & Replication Improper Input Validation Vulnerability	Veeam Backup & Replication	✗	✗	✓
CVE-2024-40714	Veeam Backup & Replication Improper TLS Certificate Vulnerability	Veeam Backup & Replication	✗	✗	✓
CVE-2024-40712	Veeam Backup & Replication Path Traversal Vulnerability	Veeam Backup & Replication	✗	✗	✓

Vulnerability Details

#1

CVE-2024-40711 is a critical Remote Code Execution (RCE) vulnerability in Veeam Backup & Replication (VBR) software, used by enterprises for backup management. This vulnerability allows unauthenticated attackers to execute arbitrary code remotely, potentially granting them full control over affected systems.

#2

The attack can trigger through the Veeam.Backup.MountService.exe by exploiting the URI /trigger on port 8000, allowing the creation of a local admin account. The exploit also utilizes net.exe to further execute malicious commands. Once exploited, attackers often create a local admin account named "point", which grants them elevated privileges to manipulate the system.

#3

Recent attacks have leveraged this flaw to deploy ransomware like Fog and Akira. These attacks begin by compromising VPN gateways, often due to missing multifactor authentication (MFA) or outdated software versions. Once inside, attackers deploy ransomware or steal data using tools like rclone, as seen in incidents involving unprotected Hyper-V servers.

#4

Additionally, five other vulnerabilities, though less severe, have been resolved with the latest update from Veeam. A proof-of-concept (PoC) exploit for CVE-2024-40711 has been made publicly available, increasing the urgency for organizations to apply the latest updates. Unpatched systems and unsupported VPNs running without MFA are at higher risk. Organizations using Veeam Backup & Replication are strongly advised to update to the latest version (12.2.0.334 or later) immediately to protect against potential attacks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-40711	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	CWE-502
CVE-2024-40713	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	CWE-287
CVE-2024-40710	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	CWE-522
CVE-2024-39718	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-40714	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	CWE-295
CVE-2024-40712	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Apply Patches and Updates: pply the latest security patch (version 12.2.0.334 or later) immediately to mitigate the CVE-2024-40711 vulnerability and other identified issues. Delayed updates leave systems exposed to exploitation. Establish a routine for checking and applying updates to all software, especially critical systems like backup solutions.

Strengthen Authentication: Enable multifactor authentication (MFA) for all admin and remote access points to add a strong security layer. Review user permissions, limiting administrative access to essential personnel. Use strong, unique passwords and update them regularly.

Secure Network Access: Restrict access to critical services by configuring firewalls to limit traffic, especially on port 8000. Use network segmentation to isolate backup systems from other parts of the network. Disable unnecessary services to reduce potential attack vectors.

Monitor and Audit Systems: Implement log monitoring to track access attempts and detect suspicious activity in real-time. Set up alerts for critical events, such as failed login attempts or unauthorized access. Regularly audit Veeam configurations to ensure security best practices are followed.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA0042 Resource Development	TA0040 Impact	TA0002 Execution
TA0008 Lateral Movement	TA0001 Initial Access	TA0010 Exfiltration	TA0003 Persistence
T1078 Valid Accounts	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1203 Exploitation for Client Execution
T1588 Obtain Capabilities	T1588.005 Exploits	T1486 Data Encrypted for Impact	T1210 Exploitation of Remote Services
T1548 Abuse Elevation Control Mechanism	T1567 Exfiltration Over Web Service	T1078.003 Local Accounts	T1136.001 Local Account
T1136 Create Account	T1133 External Remote Services	T1588.004 Digital Certificates	T1059 Command and Scripting Interpreter
T1021.001 Remote Desktop Protocol	T1021 Remote Services		

Patch Details

Upgrade to Veeam Backup & Replication version 12.2.0.334 or later.

Link:
https://www.veeam.com/kb4600

References

https://www.veeam.com/kb4649

https://labs.watchtowr.com/veeam-backup-response-rce-with-auth-but-mostly-without-auth-cve-2024-40711-2/

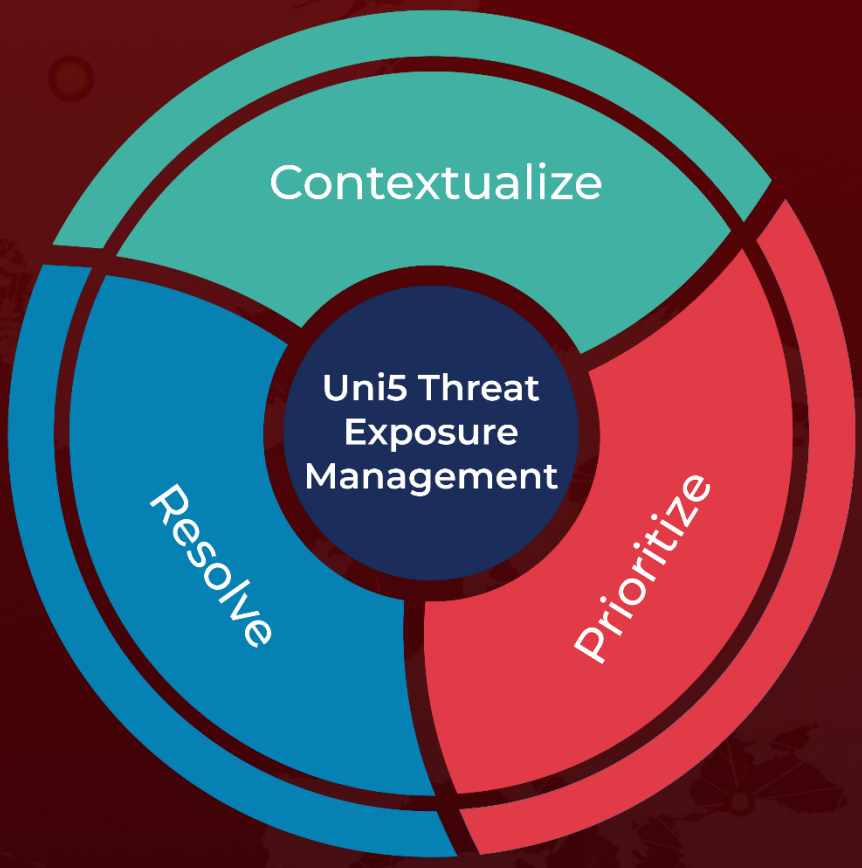
https://github.com/watchtowrlabs/CVE-2024-40711

https://infosec.exchange/@SophosXOps/113284564225476186

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 11, 2024 • 4:30 AM

More at www.hivepro.com