

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Veeam Backup & Replication RCE Flaw Opens Door for Ransomware Attacks

Date of Publication

October 11, 2024

Admiralty Code

A1

TA Number

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 These attacks begin by compromising VPN gateways, often due to missing multifactor authentication (MFA) or outdated software versions.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:*.~*.~*.~*.~*.~*.~*	
CVE-2024-40713	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_&_replication:*.~*.~*.~*.~*.~*.~*	
CVE-2024-40710	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_&_replication:*.~*.~*.~*.~*.~*.~*	
CVE-2024-39718	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_&_replication:*.~*.~*.~*.~*.~*.~*	
CVE-2024-40714	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_&_replication:*.~*.~*.~*.~*.~*.~*	
CVE-2024-40712	Veeam Backup & Replication before 12.2.0.334 versions	cpe:2.3:a:veeam:veeam_backup_&_replication:*.~*.~*.~*.~*.~*.~*	

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

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

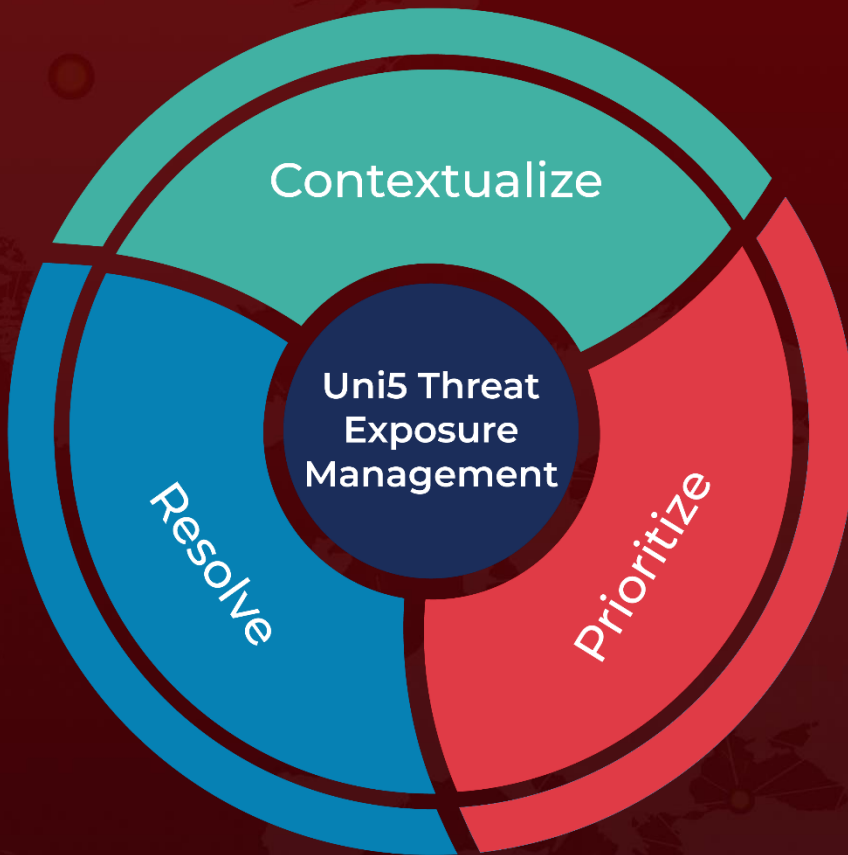
<https://github.com/watchtowrlabs/CVE-2024-40711>

<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

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com