

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Veeam Recovery Orchestrator Flaw Enables Forge of Valid JWT Tokens

Date of Publication

June 14, 2024

Admiralty Code

A1

TA Number

TA2024231




Summary

First Seen: June 11, 2024

Affected Products: Veeam Recovery Orchestrator

Impact: A critical authentication bypass vulnerability in Veeam Recovery Orchestrator, tracked as CVE-2024-29855, has been disclosed. This vulnerability poses a serious security risk by allowing unauthorized attackers to access the Veeam Recovery Orchestrator web interface (UI) with administrative privileges. Furthermore, a proof-of-concept (PoC) exploit is now available, heightening the urgency for organizations to apply mitigations promptly.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-29855	Veeam Recovery Orchestrator Authentication Bypass Vulnerability	Veeam Recovery Orchestrator			

Vulnerability Details

#1

Veeam has identified and addressed a critical security flaw in Veeam Recovery Orchestrator, identified as CVE-2024-29855, which has a severity score of 9.0 on the CVSS scale. This vulnerability enables attackers to bypass authentication and obtain administrative access to the Veeam Recovery Orchestrator web interface.

#2

The vulnerability occurs because the JWT (JSON Web Token) secret used to generate authentication tokens was hardcoded. This oversight enables attackers to create valid tokens for any user, not just administrators, granting them unauthorized access to the Veeam Recovery Orchestrator.

#3

To mitigate this risk, Veeam strongly advises users to upgrade to the patched versions: 7.1.0.230 and 7.0.0.379. These updates address the vulnerability CVE-2024-29855 by removing the hardcoded JWT secret and implementing secure token generation practices.

#4

It's crucial to note that exploiting CVE-2024-29855 requires knowledge of a valid username and role, as well as targeting a user with an active session. Attackers may also attempt a brute-force method to obtain a matching session token, further emphasizing the importance of applying security updates promptly.

#5

Given the availability of public exploits for CVE-2024-29855, there is an increased risk of attackers targeting vulnerable systems. Therefore, organizations are strongly advised to install the necessary updates immediately to protect against potential security breaches.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-29855	Veeam Recovery Orchestrator (VRO) version 7.0.0.337	cpe:2.3:a:veeam:recovery_orchestrator:*:*:*:*:*:*	CWE-287

Recommendations



Update: To mitigate this risk, it is essential to update to the patched versions 7.1.0.230 and 7.0.0.379. Regularly check for updates and apply them promptly to ensure that your system is protected against known vulnerabilities.



Implement Intrusion Detection/Prevention Systems (IDS/IPS): Use IDS/IPS to detect and prevent attempts to bypass authentication or unauthorized access attempts.



Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0043</u> Reconnaissance	<u>TA0004</u> Privilege Escalation	<u>TA0006</u> Credential Access
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1110</u> Brute Force
<u>T1591</u> Gather Victim Org Information	<u>T1591.004</u> Identify Roles		

Patch Details

Veeam has addressed the flaw and recommends upgrading to the patched versions 7.1.0.230 and 7.0.0.379 to mitigate the security risk.

Links:

<https://www.veeam.com/kb4585>

References

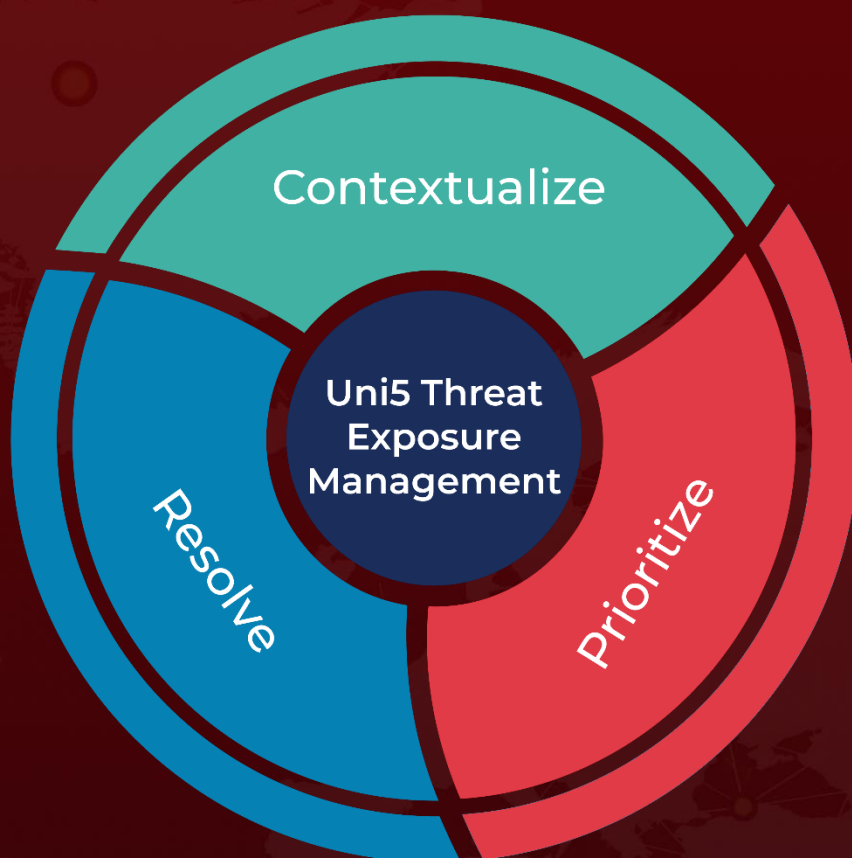
<https://summoning.team/blog/veeam-recovery-orchestrator-auth-bypass-cve-2024-29855/>

<https://github.com/sinsinology/CVE-2024-29855>

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

June 14, 2024 • 5:45 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com