Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Web Shell Threat in Commvault: Patch CVE-2025-3928 Now

Date of Publication	Admiralty Code	TA Number
April 30, 2025	A1	TA2025133

Summary

First Seen: February 20, 2025
Affected Products: Commvault
Affected Platforms: Windows, Linux
Impact: A high-severity vulnerability in Commvault's Web Server (CVE-2025-3928) is now being actively exploited in the wild. The flaw allows authenticated attackers to remotely plant web shells and execute malicious code on both Windows and Linux systems. While the exploit requires valid credentials, successful attacks can lead to full system compromise making it critical for organizations to patch immediately and review access controls.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-3928	Commvault Web Server Unspecified Vulnerability	Commvault	✓	✓	✓

Vulnerability Details

#1 Commvault has fixed a high-severity security flaw tracked as CVE-2025-3928 that could let attackers with valid credentials plant web shells and run harmful code on target servers. The issue lies within the Commvault Web Server, a key part of Commvault's enterprise backup and disaster recovery suite used by many organizations.

#2 This vulnerability affects both Windows and Linux systems and can be exploited remotely by a logged-in user. By sending specially crafted requests to the server, an attacker could take full control of the system, potentially stealing data, spreading malware, or disrupting operations.

#3 Although the technical details of the flaw haven't been publicly shared, it's serious enough that organizations to treat it as a critical threat. Exploitation could lead to a complete system compromise if left unpatched. Importantly, the flaw cannot be exploited without valid credentials, so it doesn't allow anonymous attacks. Still, any organization running older versions of Commvault software is at risk and should apply the latest updates immediately.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-3928	Commvault Version 11.36.0 - 11.36.45, 11.32.0 - 11.32.88, 11.28.0 - 11.28.140, 11.20.0 - 11.20.216	cpe:2.3:a:commvault:commvault:*:*:*:*:*:*:*:*	-

Recommendations

Patch Immediately: Update Commvault Backup & Recovery software to the latest version that fixes CVE-2025-3928. Don't delay prioritize this patch to close the door on potential remote attacks.

Restrict Access to the Commvault Web Server: Limit who can access the Commvault Web Server. Only allow trusted, internal users, and consider putting the service behind a VPN or zero trust access layer.

Audit User Accounts and Permissions: Since the exploit requires valid credentials, review user accounts in your Commvault environment. Revoke unnecessary access and enable strong authentication methods, such as MFA.

Monitor for Suspicious Activity: Keep an eye out for strange or unauthorized behavior, such as unexpected uploads or web shell activity. Set up alerts for abnormal web server traffic and new file creation in sensitive directories.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1505** Server Software Component	**T1505.003** Web Shell
T1059 Command and Scripting Interpreter	**T1078** Valid Accounts		

Patch Details

Update your Commvault Web Server to the latest version to address the Flaw. Update to the following Versions for Windows and Linux platforms.

Versions 11.36.46, 11.32.89, 11.28.141, and 11.20.217

Link: https://documentation.commvault.com/11.20/download_software.html

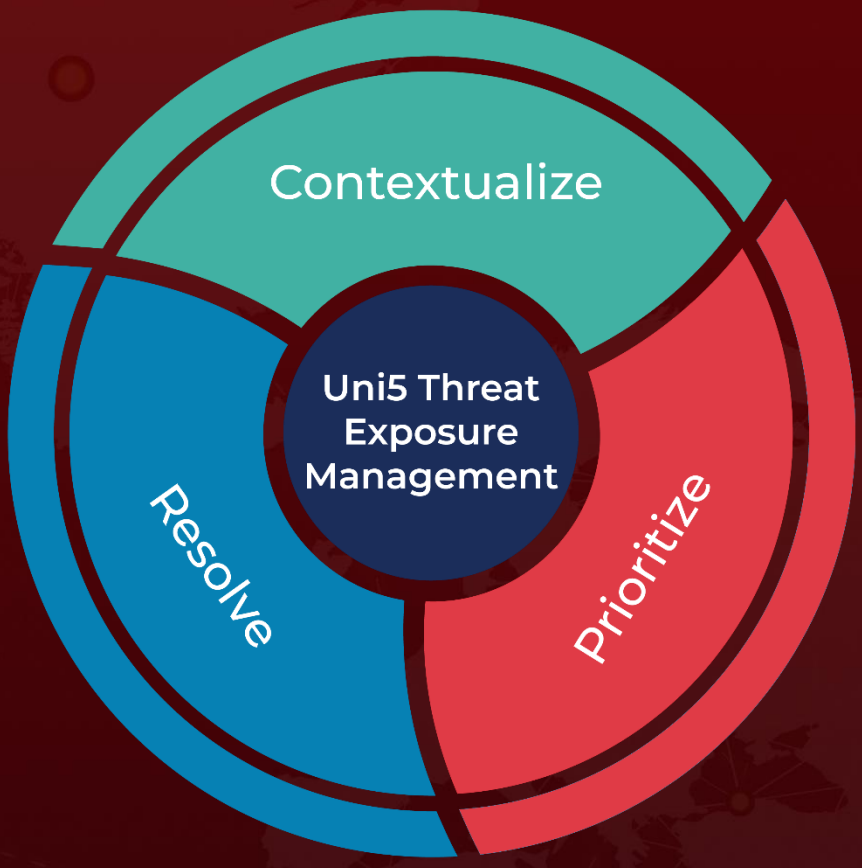
References

https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html

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

April 30, 2025 • 6:00 AM

More at www.hivepro.com