Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-37164: Critical RCE in HPE OneView Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
January 09, 2026	A1	TA2026009

Summary

First Seen: December 16, 2025
Affected Products: Hewlett Packard Enterprise (HPE) OneView
Impact: CVE-2025-37164 is a critical, unauthenticated remote code execution vulnerability in HPE OneView that allows attackers to fully compromise the management platform over the network. With a CVSS score of 10.0 and publicly available exploits, the flaw poses an immediate and severe risk to enterprise infrastructure. Successful exploitation can lead to complete control over servers, storage, and network resources managed by OneView. HPE has released fixes in OneView version 11.0 and applicable hotfixes for earlier versions. Immediate patching and restriction of management interface access are strongly recommended.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-37164	Hewlett Packard Enterprise OneView Code Injection Vulnerability	Hewlett Packard Enterprise (HPE) OneView	✗	✓	✓

Vulnerability Details

#1 CVE-2025-37164 is a critical remote code execution (RCE) vulnerability affecting HPE OneView, a centralized infrastructure management platform widely used in enterprise data centers. The flaw allows an unauthenticated remote attacker to execute arbitrary code over the network, requiring no user interaction or credentials. Due to OneView's privileged role in managing servers, storage, and networking, successful exploitation can lead to a full compromise of managed infrastructure.

#2 The vulnerability impacts HPE OneView versions prior to 11.0, with a CVSS score of 10.0, reflecting maximum severity. The attack complexity is low, making exploitation accessible even to less sophisticated threat actors. Public proof-of-concept exploits are available, and the vulnerability has been reported as actively exploited in the wild, significantly increasing real-world risk.

#3 From an impact perspective, attackers could gain complete control over the OneView appliance, manipulate infrastructure configurations, deploy malware, establish persistence, or disrupt critical services. Because OneView often sits in trusted management networks, exploitation may also enable lateral movement into otherwise segmented environments.

#4 HPE has addressed the issue by releasing fixes in OneView 11.0 and hotfixes for affected earlier versions. Notably, HPE confirmed no workarounds exist, patching is the only remediation path. Organizations are strongly advised to patch immediately or upgrade where possible. As interim mitigations, access to OneView management interfaces should be tightly restricted and monitored until remediation is complete.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-37164	HPE OneView (Before 11.0)	cpe:2.3:a:hpe:oneview:*:*:*:*:*:*:*:*	CWE-94

Recommendations

Upgrade to HPE OneView Version 11.0: Organizations should prioritize upgrading to HPE OneView version 11.0, which addresses the vulnerability by removing access to the vulnerable API endpoint. This upgrade represents the most comprehensive remediation approach and is strongly recommended for all affected deployments to ensure long-term protection against this and potentially related vulnerabilities.

Apply Emergency Security Hotfixes: For organizations unable to immediately upgrade to version 11.0, HPE has released emergency hotfixes that must be applied without delay. The HPE OneView Virtual Appliance hotfix (HPE_OV_CVE_37164_Z7550-98077) and the HPE Synergy CVE Security Hotfix are available through HPE's official portals. It is critical to note that these hotfixes must be reapplied after upgrading HPE OneView from version 6.60.xx to 7.00.00, including after any HPE Synergy Composer reimage operations.

Implement Network Segmentation and Access Controls: Restrict network access to HPE OneView management interfaces to trusted IP addresses only and ensure that management platforms are not exposed to the internet or untrusted network segments. Implementing strict network segmentation around critical infrastructure management systems reduces the attack surface and limits potential exploitation vectors even when patches cannot be immediately applied.

Conduct Forensic Analysis on Vulnerable Systems: Given the confirmed active exploitation of this vulnerability, organizations should conduct thorough forensic analysis on any HPE OneView systems that may have been exposed prior to patching. Review access logs for suspicious activity, particularly any unusual requests to the /rest/id-pools/executeCommand endpoint, and investigate any indicators of unauthorized access or system modification.

Rotate Credentials and Secrets: As a precautionary measure following remediation, rotate any credentials, API keys, certificates, or secrets that may have been accessible from compromised HPE OneView systems. This includes credentials for managed infrastructure components, administrative accounts, and any integrated systems that HPE OneView has access to manage.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Links

https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US
https://myenterpriselicense.hpe.com/cwp-ui/product-details/HPE_OV_CVE_37164_Z7550-98077/-/sw_free
https://support.hpe.com/connect/s/softwaredetails?collectionId=MTX-64daeb5ed0df44a0&tab=releaseNotes

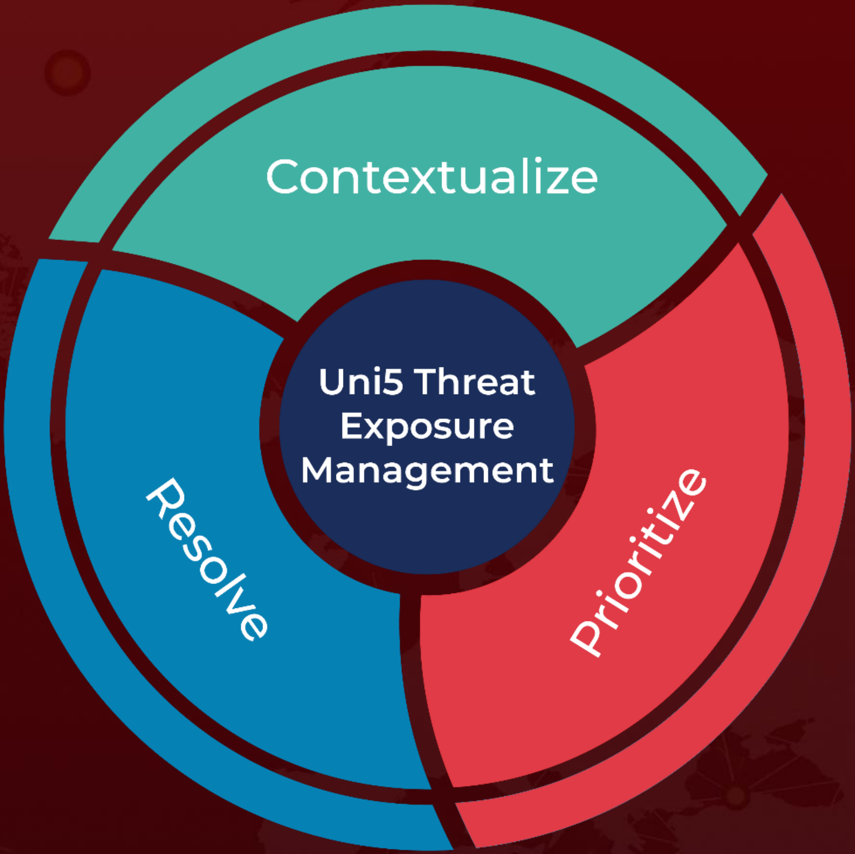
References

https://www.rapid7.com/blog/post/etr-cve-2025-37164-critical-unauthenticated-rce-affecting-hewlett-packard-enterprise-oneview/
https://github.com/rapid7/metasploit-framework/pull/20792
https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US#vulnerability-summary-1

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

January 09, 2026 • 09:30 AM

More at www.hivepro.com