THREAT BULLETINS

Active Exploitation of Critical HPE OneView RCE Flaw (CVE-2025-37164)

TLP:WHITE

Jan 08, 2026

A maximum-severity vulnerability in HPE OneView, tracked as CVE-2025-37164, is being actively exploited in the wild.

This unauthenticated remote code execution (RCE) flaw carries a CVSS score of 10.0, allowing attackers to gain full control of data center infrastructure management systems. Organizations are urged to prioritize the immediate application of available security updates or hotfixes to mitigate the risk of compromise.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their level of risk to this vulnerability.

Analysis

The security flaw was publicly disclosed by Hewlett Packard Enterprise (HPE) on December 16, 2025, following a report by a third-party security researcher. The vulnerability is a code injection flaw located in an unsecured REST API endpoint (/rest/id-pools/executeCommand) within the HPE OneView management

software. This specific endpoint fails to enforce any authentication and is directly accessible to any remote attacker with network access to the OneView management plane.

Exploiting this flaw allows an unauthenticated remote attacker to execute arbitrary commands with elevated privileges on the targeted system. Given that HPE OneView acts as a centralized control plane for deploying and managing physical servers, storage, and networking hardware, successful exploitation can grant an adversary control over critical components of data center infrastructure. Threat actors can use this access to modify configurations, deploy malicious workloads, or exfiltrate sensitive data while bypassing standard application-level logging.

The vulnerability affects a broad range of HPE OneView versions, specifically all releases before version 11.00. This includes virtual appliances and HPE Synergy Composer instances ranging from version 5.20 through 10.20. The release of a detailed proof-of-concept (PoC) exploit and a subsequent Metasploit module in late December 2025 significantly lowered the barrier to entry for attackers, leading to the confirmed reports of opportunistic exploitation observed across global networks in early January 2026.

HPE has addressed the flaw by releasing HPE OneView version 11.00, which fully resolves the issue. For organizations that cannot perform a full version upgrade immediately, HPE has also provided security hotfixes specifically for versions 5.20 through 10.20. There are no known configuration-based workarounds that provide equivalent protection; therefore, applying vendor-supplied updates or hotfixes is the only reliable defense against this threat.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

1. Apply security updates to upgrade HPE OneView to version 11.00 or later.
2. If a full upgrade is not possible, apply the specific security hotfix for your platform:
    - Install the hotfix for HPE OneView Virtual Appliance
    - Install the hotfix for HPE Synergy Composer
3. Note - that the hotfix must be reapplied after an appliance upgrade from version 6.60.x to 7.00.00, or after any HPE Synergy Composer re-imaging operations.
4. Limit network-level access to the OneView management interface to trusted administrative subnets only.
    - Management consoles should never be exposed directly to the public internet.
5. Check for unauthorized administrator accounts or unusual API requests targeting the /rest/id-pools/executeCommand endpoint to identify potential historic compromise.
6. Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	hpe, github, hpe 1, rapid7, hhs, nist, hpe 2

Alert ID 60685868

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-37164, HPE OneView

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**