Smarttech
YOUR 24/7 SECURITY PARTNER

Critical VMware vCenter Flaw Now Exploited by Ransomware Groups

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	163
Authors	Dorin Constantin Banu < constatin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-15
Issue Date	2026-09-15

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

A critical remote code execution vulnerability affecting VMware vCenter is under active exploitation by ransomware groups. The vulnerability allows unauthenticated attackers with network access to execute arbitrary code on vulnerable servers, making immediate patching a top priority for organizations using VMware vCenter.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

On July 29, Broadcom patched CVE-2026-59310, a critical VMware vCenter Syslog Server vulnerability that was subsequently exploited by a suspected APT actor to deploy a reverse SSH backdoor for persistence and remote access. Shortly after disclosure, researchers identified 361 compromised IP addresses across 47 countries, highlighting the rapid weaponization of the vulnerability and prompting CISA to add it to its Known Exploited Vulnerabilities (KEV) Catalog. More recently, CISA updated the KEV entry to confirm that ransomware groups are now actively exploiting the flaw.

Shadowserver currently tracks more than 450 internet-exposed VMware vCenter servers. However, there is currently no public data indicating how many of these systems have been patched against CVE-2026-59310.

Recommendations

Smarttech247 team recommend the following actions be taken:

- Apply the appropriate patches or appropriate mitigations provided by VMware to vulnerable systems immediately after appropriate testing.

- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Kindly ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

https://www.bleepingcomputer.com/news/security/cisa-critical-vmware-vcenter-rce-flaw-now-exploited-by-ransomware-gangs/

CVE

CVE-2026-59310

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com