GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

19 August 2026

Advisory 191: CVE-2026-59310_Broadcom VMware vCenter Path Traversal Vulnerability

Release Date: 29th July 2026 (Added 18 August 2026)
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-59310 is a critical-severity directory traversal vulnerability in the Syslog server component of VMware vCenter Server, disclosed by Broadcom on 29 July 2026. It carries a CVSS Base Score of 9.8 and allows an unauthenticated attacker with network access to vCenter to execute arbitrary code on the appliance. Broadcom has confirmed no workaround exists for this vulnerability; patching is the only remediation.

What are the systems affected?

Affected systems include all currently supported VMware vCenter Server branches. vCenter is the central management plane for a VMware virtualised environment, so compromise gives an attacker a foothold across every ESXi host and virtual machine it manages.

VMware vCenter Server 9.1.x - (Affected, fixed in 9.1.0.0300)
VMware vCenter Server 9.0.x - (Affected, fixed in 9.0.2.0100)

VMware vCenter Server 8.0 - (Affected, fixed in 8.0 U3k or 8.0 U2f, branch-dependent)
VMware Cloud Foundation (vCenter 5.x component) - (Affected, async patch to 8.0 U3k)
VMware Telco Cloud Platform and Infrastructure - (Affected, see KB449886)

Any organisation running vCenter reachable from the internet, or on an unsegmented internal network, faces critical risk given confirmed active exploitation and the absence of any workaround.

What does this mean?

This flaw requires no initial access step: network reachability to vCenter is the only prerequisite, and the observed campaign moved from disclosure to compromise in five days.

Step 1 - Unauthenticated Directory Traversal
The attacker sends crafted requests to the vCenter Syslog server that escape the intended directory due to insufficient path sanitisation, requiring only network access to the appliance.

Step 2 - Arbitrary Code Execution
The traversal is leveraged to write or execute attacker-controlled code on the vCenter appliance, achieving remote code execution with no credentials or user interaction required.

Step 3 - Persistence via Reverse SSH
Observed intrusions deploy a malicious cron job alongside the open-source reverse_ssh tool, establishing a persistent backdoor to attacker-controlled infrastructure that survives a simple reboot.

Step 4 - Lateral Movement and Cover
With control of vCenter - the central management plane for the entire virtualised environment - the attacker gains a foothold to pivot into ESXi hosts and virtual machines. Observed cases include deployment of **Babuk-derived ransomware**, assessed by investigators as a likely decoy intended to destroy forensic evidence rather than a genuine extortion attempt.

Mitigation process

CERTVU recommends the following:

Apply the Broadcom Patch Immediately (No Workaround Exists)

Update vCenter Server to 9.1.0.0300, 9.0.2.0100, or 8.0 U3k/U2f depending on the deployed branch, per VMSA-2026-0006.1. VMware Cloud Foundation and Telco Cloud customers should follow the async patch guidance in the relevant KB. Broadcom has confirmed no workaround exists for CVE-2026-59310, so patching is the only remediation; given confirmed active exploitation by a nation-state-linked actor, treat this as an emergency change rather than a scheduled one, prioritising any vCenter instance reachable from the internet or from an unsegmented internal network.

Broadcom Security Advisory VMSA-2026-0006.1

Reference

1. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017
2. https://www.cve.org/CVERecord?id=CVE-2026-59310
3. https://thehackernews.com/2026/08/attackers-exploit-vmware-vcenter.html
4. https://www.shadowserver.org/what-we-do/network-reporting/vmware-vcenter-cve-2026-59310-exploitation-victim-special-report/

.