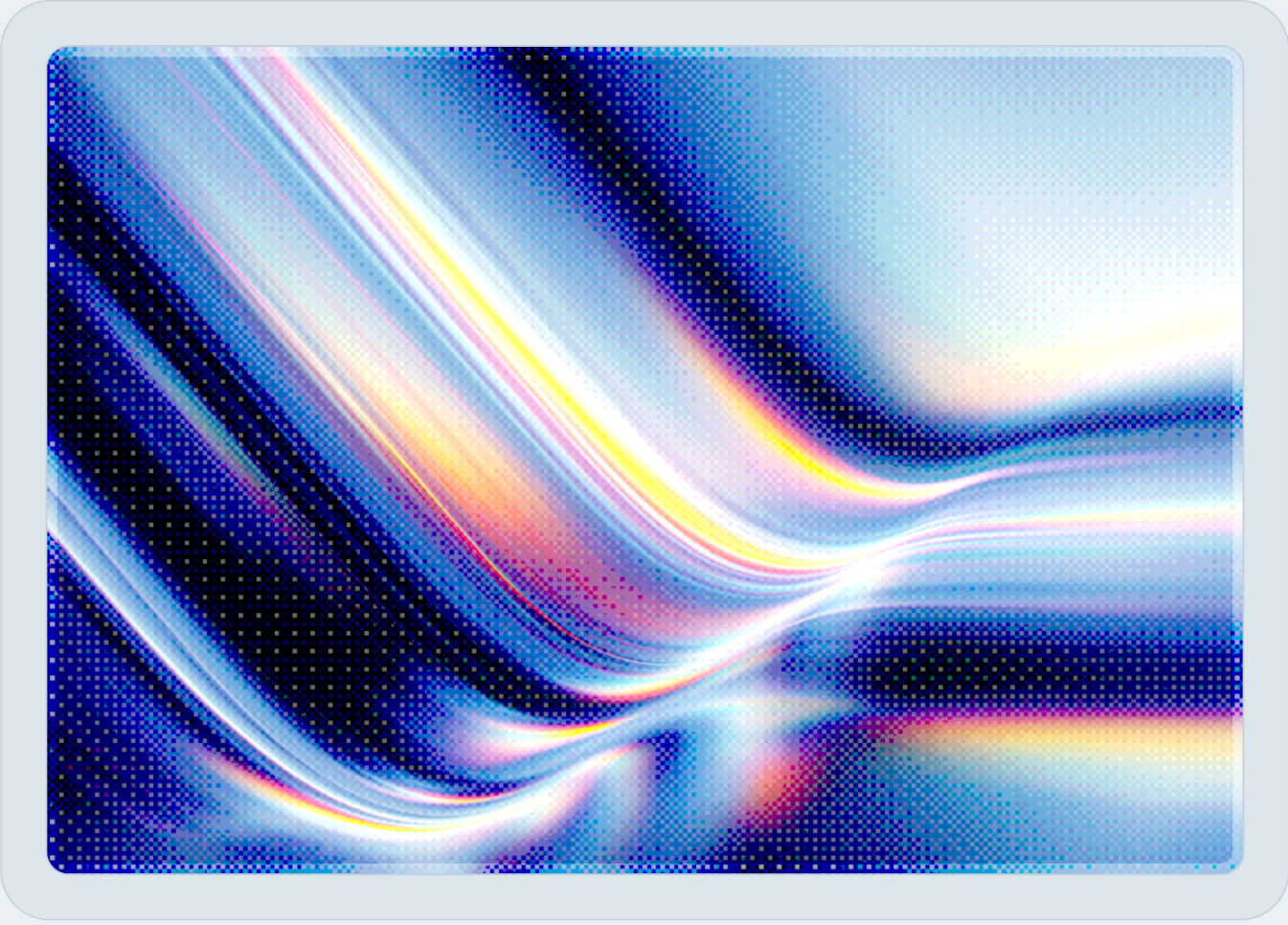
CSAI Foundation | Cloud Security Alliance

VMware vCenter Directory Traversal Under Active Global Exploitation

CVE-2026-59310: 361 Victim IPs Across 47 Countries via Reverse SSH Backdoors

2026-08-13

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

A critical-severity directory traversal vulnerability in the VMware vCenter Server Syslog service, tracked as CVE-2026-59310 and carrying a CVSS v3.1 base score of 9.8 out of a maximum 10.0 [2][3], is being actively exploited by a suspected advanced persistent threat actor to gain unauthenticated remote code execution on internet- and network-exposed vCenter instances. Broadcom disclosed the flaw in advisory VMSA-2026-0006 on July 29, 2026, alongside a companion authentication bypass in the VMware Directory Service, CVE-2026-59309, which also scores 9.8 [2][3]. German incident-response firm QUIRSO GmbH identified live exploitation beginning August 3, 2026, just five days after disclosure, and as of its August 10 report had catalogued 361 unique victim IP addresses spanning 47 countries — a figure likely to have grown further in the days since — with Germany, the United States, Turkey, Iran, and France accounting for roughly half the observed victims [6]. Attackers use the path traversal flaw to write and execute arbitrary code on the vCenter appliance, then plant cron jobs that launch reverse_ssh, an open-source reverse-shell framework, establishing outbound command-and-control channels that evade defenses built primarily to inspect inbound traffic [4][5][6]. Because vCenter functions as the central control plane for VMware virtualization environments, successful exploitation gives an attacker authority over every managed host, virtual machine, and snapshot, making rapid patching to the fixed builds — 9.1.0.0300, 9.0.2.0100, or 8.0 U3k/U2f — the only effective remediation, since Broadcom has confirmed no workaround exists [2][3].

Background

VMware vCenter Server is the management plane that administrators use to configure, monitor, and orchestrate ESXi hosts and the virtual machines running on them across an organization's private cloud and data center infrastructure. Because vCenter sits at the top of the virtualization stack with broad administrative reach into every workload it manages, it has long been viewed as a high-value target for ransomware operators and state-linked intrusion sets, consistent with its roughly ten prior appearances on CISA's Known Exploited Vulnerabilities catalog, as Rapid7 has noted [1]. On July 29, 2026, Broadcom published security advisory VMSA-2026-0006, disclosing five vulnerabilities across VMware ESX, vCenter Server, Workstation, and Fusion, with individual CVSS scores ranging from 2.7 to 9.8 [2][3].

Two of the five issues stand out for their severity and reach. CVE-2026-59309 is an authentication bypass in the VMware Directory Service (VMDir), the identity and authentication backbone underpinning vCenter's single sign-on, that lets a threat actor with mere network access to a vulnerable appliance obtain unauthorized administrative access without any credentials [2][3]. CVE-2026-59310, the subject of this note, is a directory traversal flaw in vCenter's Syslog server that permits an unauthenticated, network-adjacent attacker to manipulate file paths and write files outside their intended directory, ultimately achieving arbitrary code execution on the appliance [1][2]. Both vulnerabilities carry a CVSS v3.1 base score of 9.8, and Broadcom's advisory states plainly that no workaround exists for either — patching is the only remediation path [2][3]. The affected product set is broad, spanning VMware Cloud Foundation 9.1.x, 9.0.x, and 5.x; VMware vSphere Foundation 9.1.x and 9.0.x; standalone VMware vCenter Server 8.0; and VMware Telco Cloud Platform and Telco Cloud Infrastructure builds used by carrier-grade environments [2][3]. Fixed versions are vCenter 9.1.0.0300, 9.0.2.0100, and 8.0 U3k (with a corresponding U2f branch fix); Broadcom updated the advisory on August 3, 2026 as VMSA-2026-0006.1 to refine remediation guidance [2][3].

At the time of initial disclosure, at least one vendor analysis reported no evidence of active exploitation or public proof-of-concept code [1]. That assessment did not hold for long: on August 10, 2026, QUIRSO GmbH published research documenting an active exploitation campaign against CVE-2026-59310 that it had uncovered during an incident-response engagement, with first observed activity dating to August 3 — the same week the advisory was updated [4][5][6]. The compressed window between disclosure and weaponization is consistent with a pattern CSA has observed elsewhere in enterprise infrastructure security: sophisticated actors reverse-engineering vendor patches or advisory details within days of publication, leaving organizations that have not yet deployed the fix exposed almost immediately.

Security Analysis

QUIRSO's telemetry shows a sharply front-loaded campaign. Exploitation activity began August 3, 2026, five calendar days after Broadcom's initial disclosure, and peaked the following day with 151 newly observed victim IP addresses in a single 24-hour period [6]. By August 5, approximately 95 percent of the eventual victim population had already appeared in the researchers' data, indicating that the actor or actors behind the campaign moved with considerable speed and automation once exploitation began, rather than probing gradually over an extended reconnaissance period [6]. As of QUIRSO's most recent update, the campaign had touched 361 unique victim IP addresses distributed across 47 countries, with Germany, the United States, Turkey, Iran, and France together accounting for 185 of the 361 total — roughly half of all observed compromises concentrated in five countries [4][5][6]. This geographic spread, combined with the speed of the initial wave, is consistent with an actor operating from a pre-built target list or internet-wide scanning infrastructure rather than manually selecting victims.

The exploitation chain itself follows a straightforward but effective pattern. An attacker with network access to the vCenter management interface sends crafted input to the Syslog server that exploits the directory traversal weakness in CVE-2026-59310, allowing the attacker to write a malicious file outside its intended directory and ultimately execute arbitrary code on the appliance [1][6]. Once code execution is achieved, QUIRSO observed the attackers deploying scheduled cron jobs that install and launch reverse_ssh, an open-source SSH-based reverse-shell framework, to establish a persistent outbound connection to attacker-controlled infrastructure [4][5][6]. This reverse-shell approach functions as an effective evasion technique, whether or not deliberately chosen for that purpose: because the connection is initiated from inside the compromised environment outward to the attacker, it bypasses network security controls that are tuned to inspect and restrict inbound traffic but give comparatively little scrutiny to outbound SSH sessions, particularly from infrastructure servers, which security teams often monitor less closely than end-user endpoints — a common blind spot in outbound-traffic visibility [5][6]. QUIRSO researchers have characterized the operation as likely the work of an advanced persistent threat actor, suggesting the group may have had insight into the vulnerability prior to public disclosure even though the disclosure event itself appears to have served as the practical trigger for the campaign's launch [4][6].

The consequences of a successful compromise extend well beyond the vCenter appliance itself. Because vCenter is the administrative control point for an organization's entire virtualization estate, an attacker who achieves code execution on it effectively gains the ability to manipulate every host, every running virtual machine, and every stored snapshot that vCenter manages [5]. That level of access theoretically opens a path to follow-on objectives common in ransomware and espionage operations alike — though QUIRSO's reporting does not indicate that any of these outcomes have yet been observed in this specific campaign — including mass encryption or destruction of VM disk files at the hypervisor layer (which bypasses guest-level endpoint protection entirely), theft of sensitive data from any hosted workload, deployment of additional backdoors across managed hosts, and disruption of backup and recovery infrastructure if it is itself virtualized. QUIRSO has published a YARA detection rule via its GitHub repository to help defenders identify reverse_ssh artifacts associated with the campaign and has stated it is coordinating additional indicators of compromise with law enforcement, with further analysis expected in follow-up reporting [6].

The table below summarizes the two most severe vulnerabilities disclosed in VMSA-2026-0006, both of which affect the same underlying product set and share the same remediation path.

CVE	Component	Vulnerability Type	CVSS v3.1	Authentication Required	Status as of Aug 13, 2026
CVE-2026-59309	VMware Directory Service (VMDir)	Authentication bypass	9.8	None	No confirmed public exploitation reported to date
CVE-2026-59310	vCenter Syslog Server	Directory traversal → arbitrary code execution	9.8	None	Actively exploited since August 3, 2026

Recommendations

Immediate Actions

Organizations running any affected vCenter, Cloud Foundation, vSphere Foundation, or Telco Cloud product should treat patching as the top infrastructure priority this week, not a routine maintenance-window item, given that Broadcom has confirmed no workaround exists for CVE-2026-59310 [2][3]. Update vCenter Server to 9.1.0.0300, 9.0.2.0100, or 8.0 U3k/U2f as appropriate to the deployed branch, following Broadcom's guidance in VMSA-2026-0006.1, and apply the corresponding fixes for co-managed Telco Cloud Platform and Telco Cloud Infrastructure deployments referenced in the advisory's supplemental knowledge base article [2][3]. Security teams should also immediately hunt for indicators associated with this campaign: unexpected cron or scheduled-task entries on the vCenter appliance, unfamiliar SSH binaries or processes matching the reverse_ssh tool, and outbound network connections from vCenter to unfamiliar external hosts over SSH or SSH-like ports. QUIRSO's published YARA rule provides a starting point for this hunt and should be run against vCenter appliance file systems and any centralized log aggregation covering vCenter hosts [6].

Short-Term Mitigations

Because both critical flaws in VMSA-2026-0006 are exploitable by any actor with mere network access and no credentials, organizations should restrict network reachability to vCenter management interfaces to only the administrative jump hosts, bastion systems, or VPN segments that require it, rather than leaving management planes reachable from general enterprise or internet-facing networks. Given that CVE-2026-59309 separately allows authentication bypass against the same product family, teams that patch should also review VMDir-related authentication logs for anomalous administrative sessions predating the patch and consider rotating vCenter administrative credentials as a precaution. Enhanced logging and monitoring of the vCenter appliance and its Syslog service — including forwarding vCenter logs to an external, tamper-resistant SIEM rather than relying solely on local retention that an attacker with code execution could alter — will materially improve detection of both this campaign and future attempts against the same infrastructure. Firewall and network policy reviews should specifically examine whether outbound SSH or similarly disguised traffic from infrastructure servers is permitted and monitored, since the reverse_ssh technique specifically exploits the common asymmetry between inbound and outbound traffic scrutiny.

Strategic Considerations

This campaign reinforces that virtualization management planes deserve the same patch-management urgency and network isolation discipline typically reserved for internet-facing applications, given how directly they translate into blast radius: a single compromised vCenter instance can expose an entire virtualized data center. Organizations should incorporate hypervisor and virtualization-management infrastructure explicitly into vulnerability management SLAs that mandate expedited patching for critical, unauthenticated, network-exploitable findings, rather than treating infrastructure software on the same cadence as lower-risk internal tooling. The five-day gap between disclosure and observed exploitation in this campaign — and the fact that roughly 95 percent of eventual victims were compromised within the first two days of active exploitation — is a stark illustration of how quickly a high-value infrastructure target can be weaponized once a patch is public, and should inform tabletop exercises and incident-response readiness planning specifically scoped to hypervisor-layer compromise. Finally, because vCenter's historical presence on CISA's Known Exploited Vulnerabilities catalog long predates this incident, organizations relying on VMware virtualization should treat it as a persistently high-interest target for threat actors and weight it accordingly in ongoing risk assessments and vendor security reviews [1].

CSA Resource Alignment

This incident's core exploitation pattern — an unauthenticated path traversal vulnerability escalating to remote code execution against a rapidly weaponized target — mirrors CSA's prior rapid-research coverage of Langflow's path traversal vulnerability. "Langflow Path Traversal: Unauthenticated RCE Actively Exploited" analyzed CVE-2026-5027, in which attackers similarly abused unsanitized file-path handling to achieve unauthenticated arbitrary file writes and code execution, and it offers directly transferable guidance on why path traversal flaws in infrastructure-adjacent platforms escalate to full compromise so quickly and why vendor-supplied patching is typically the only durable fix when no workaround exists [7]. The co-disclosed authentication bypass in VMware Directory Service, CVE-2026-59309, parallels CSA's research note on "CVE-2026-16232: Check Point SmartConsole Authentication Bypass," which examined how an authentication-bypass flaw in an enterprise security management console allowed unauthenticated attackers to obtain administrative control and rewrite policy across every managed system from a single compromised point — the same structural risk that a VMDir bypass poses to every vCenter-managed host [8]. Both notes reinforce this document's central recommendation that management-plane vulnerabilities affecting authentication or file-handling logic warrant same-week patching regardless of whether active exploitation has yet been confirmed. More broadly, this incident maps to the vulnerability and threat management, and application and infrastructure security, domains of CSA's AI Controls Matrix (AICM) v1.1, whose control objectives around timely patching, exposure management for network-accessible administrative interfaces, and monitoring of infrastructure control planes apply equally to traditional virtualization management systems and to the AI-enabled cloud environments the framework was designed to cover [9].

References

[1] Rapid7. "Critical VMware vCenter Vulnerabilities Allow Authentication Bypass and Remote Code Execution (CVE-2026-59309, CVE-2026-59310)." Rapid7 Blog, July 2026.

[2] VMware/Broadcom. "VMSA-2026-0006 Security Advisory." VMware Cloud Foundation Security and Compliance Guidelines, July 29, 2026 (updated August 3, 2026).

[3] Broadcom. "Security Advisory: VMSA-2026-0006." Broadcom Support Portal, July 29, 2026.

[4] The Hacker News. "Attackers Exploit VMware vCenter Vulnerability to Gain Persistent Remote Access." The Hacker News, August 2026.

[5] SC World. "Critical VMware vCenter Flaw Actively Exploited in 47 Countries." SC World, August 2026.

[6] QUIRSO GmbH. "Active Exploitation of CVE-2026-59310: 361 Victim IPs Across 47 Countries." Medium, August 10, 2026.

[7] Cloud Security Alliance. "Langflow Path Traversal: Unauthenticated RCE Actively Exploited." CSA Lab Space, June 12, 2026.

[8] Cloud Security Alliance. "CVE-2026-16232: Check Point SmartConsole Authentication Bypass." CSA Lab Space, July 25, 2026.

[9] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, June 22, 2026.