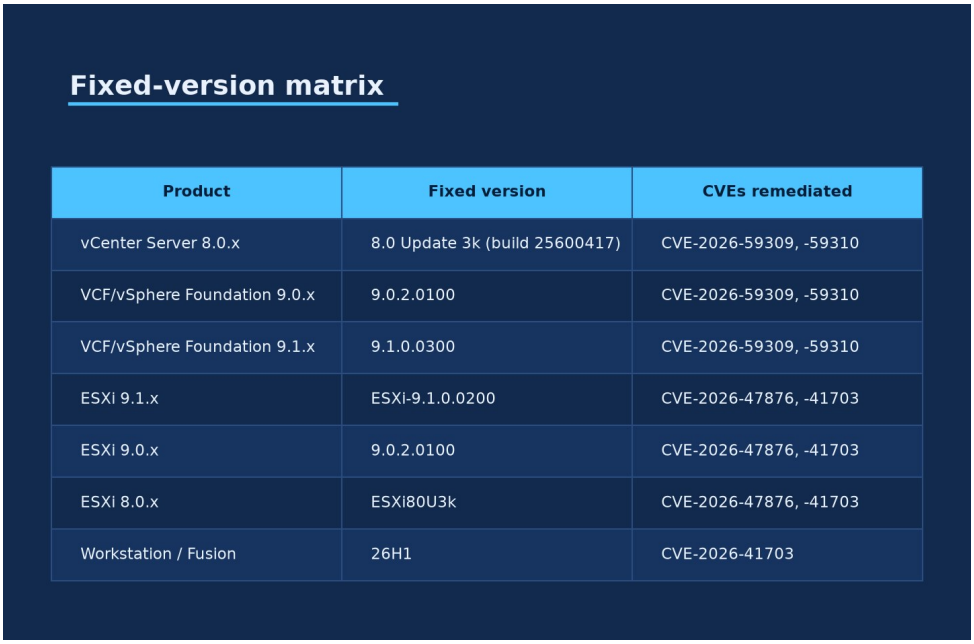
VMSA-2026-0006: Defender's Guide to the Critical vCenter Auth-Bypass (CVE-2026-59309) and Syslog Directory-Traversal RCE (CVE-2026-59310)

A researched, cited report · Ask Anything

Contents

Critical CVEs in VMSA-2026-0006 - Source: Ask Anything analysis - generated from the report's cited data

Executive summary



Product	Fixed version	CVEs remediated
vCenter Server 8.0.x	8.0 Update 3k (build 25600417)	CVE-2026-59309, -59310
VCF/vSphere Foundation 9.0.x	9.0.2.0100	CVE-2026-59309, -59310
VCF/vSphere Foundation 9.1.x	9.1.0.0300	CVE-2026-59309, -59310
ESXi 9.1.x	ESXi-9.1.0.0200	CVE-2026-47876, -41703
ESXi 9.0.x	9.0.2.0100	CVE-2026-47876, -41703
ESXi 8.0.x	ESXi80U3k	CVE-2026-47876, -41703
Workstation / Fusion	26H1	CVE-2026-41703

Fixed-version matrix - Source: Ask Anything analysis - generated from the report's cited data

On July 29, 2026, Broadcom published VMSA-2026-0006, a critical-severity advisory disclosing five vulnerabilities across the VMware Cloud Foundation, vSphere Foundation, vCenter Server, ESX/ESXi, Workstation, Fusion, Telco Cloud Platform, and Telco Cloud Infrastructure product lines. Two of the five - CVE-2026-59309 and CVE-2026-59310 - are unauthenticated, network-exploitable, CVSSv3.1 9.8/Critical vulnerabilities in vCenter Server itself, the single control-plane appliance that manages ESXi hosts, virtual machine inventory, permissions, and cluster operations across a vSphere estate. CVE-2026-59309 is an authentication bypass in the VMware Directory Service (vmdir), the LDAP-based identity backend behind vCenter Single Sign-On; NVD classifies it under CWE-303 (Incorrect Implementation of an Authentication Algorithm). CVE-2026-59310 is a directory-traversal flaw (CWE-22) in the vCenter Syslog Server component that Broadcom and downstream analysts describe as enabling arbitrary code execution on the appliance. Both carry the identical vector

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - network-reachable, low complexity, no privileges, no user interaction, full compromise of confidentiality, integrity, and availability (Broadcom Support Portal, 2026; NVD CVE-2026-59309, 2026; NVD CVE-2026-59310, 2026).

For defenders, the operationally decisive fact is this: Broadcom has stated plainly that no workarounds exist for either vulnerability, and - as of this writing - Broadcom has not published the vulnerable request path, endpoint, protocol operation, or parsing defect that causes either flaw. Independent technical review of the advisory language confirms the disclosure is deliberately narrow: it names the affected component (vmdir for CVE-2026-59309, the syslog server for CVE-2026-59310) but does not describe the mechanism, meaning any specific claim about "which port," "which API," or "which log format" is currently speculation, not vendor-confirmed fact (Penligent Hacking Labs, 2026). This is a materially different posture than, for example, the 2023 vCenter DCE/RPC heap-overflow (CVE-2023-34048), where more technical detail eventually became public. Treat vendor-silence-on-mechanism as a signal to widen detection scope rather than narrow it.

As of July 31, 2026 (two days post-disclosure), there is no confirmed evidence of in-the-wild exploitation and no public proof-of-concept exploit code for either CVE, according to Rapid7's emerging threat response, Broadcom's own advisory text, and independent trackers (Rapid7, 2026; BleepingComputer, 2026). This is consistent with - not a guarantee against - the pattern seen with prior critical vCenter vulnerabilities: Rapid7 notes that vCenter Server has appeared on CISA's Known Exploited Vulnerabilities (KEV) catalog ten separate times in past years, meaning unauthenticated, network-reachable vCenter bugs have a strong and repeated history of moving from disclosure to active exploitation, frequently within days to a few weeks once a working bypass or traversal payload is reverse-engineered from the patch diff (Rapid7, 2026). Neither CVE-2026-59309 nor CVE-2026-59310 was confirmed as CISA KEV-listed at the time of this report's research; a small number of secondary aggregators surfaced an ambiguous "added July 27, 2026" KEV date that predates the July 29 advisory publication and is very likely a data error or conflation with an unrelated KEV batch - treat that specific claim as unverified until CISA's own catalog is checked directly.

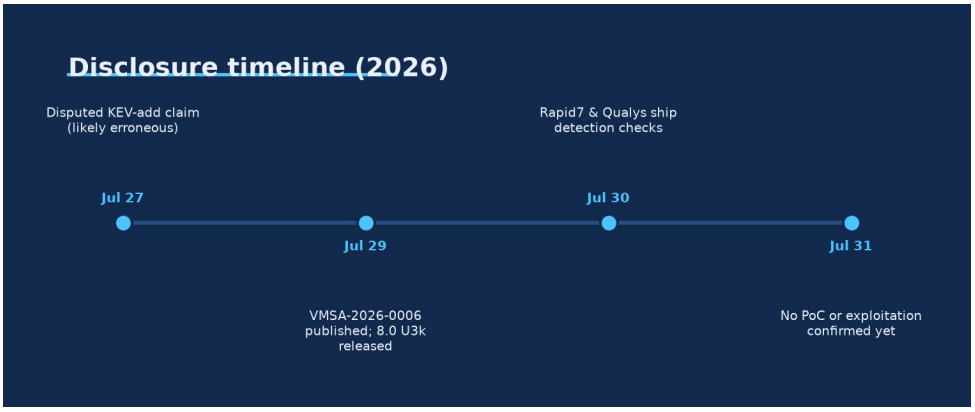
The fixed-version matrix is straightforward relative to the advisory's product sprawl: vCenter Server 8.0 Update 3k (build 25600417), VMware Cloud Foundation/vSphere Foundation 9.0.2.0100, and VMware Cloud Foundation/vSphere Foundation 9.1.0.0300 all remediate CVE-2026-59309 and CVE-2026-59310 (Broadcom Support Portal, 2026; Broadcom techdocs, 2026). A separate, easily-missed operational trap accompanies the 8.0 U3k patch: Broadcom's own release notes state that upgrading a vCenter instance to 8.0 U3k blocks the subsequent upgrade path to VMware Cloud Foundation/vSphere Foundation 9.1.0 or any 9.1.0-based patch, because 8.0 U3k contains fixes not yet present in the shipping 9.1.0 baseline and installing 9.1.0 over it would be a "back-in-time" downgrade of security content (Broadcom techdocs, 2026; AngrySysops, 2026). Any organization mid-migration to VCF 9.1 needs to sequence its patching carefully - a detail this report treats at length in Detail and Practical synthesis, because getting the order wrong can strand an estate on an unsupported upgrade path for months.

Because Broadcom has withheld the exploitation mechanism, conventional signature-based detection is not currently possible for either CVE. Rapid7 shipped unauthenticated vulnerability-presence checks

(version-fingerprinting, not exploit detection) in InsightVM, Nexpose, and Exposure Command by July 30, 2026, and Qualys published detection QIDs 388184, 216356, and 216358 the same day (Rapid7, 2026; Qualys ThreatPROTECT, 2026). In the absence of an official indicator of compromise, the credible defensive posture is behavioral: correlate vCenter SSO authentication events against upstream identity-provider logs, hunt for administrative sessions that lack a corresponding successful-authentication or MFA event, monitor vmdir for connection anomalies and TLS/SSL errors, and preserve firewall flow logs showing any inbound connection to vCenter management interfaces predating the disclosure date for retrospective hunting once more technical detail emerges (Penligent Hacking Labs, 2026).

This report treats CVE-2026-59309 and CVE-2026-59310 as the primary subject per the request, and covers the three co-disclosed CVEs (CVE-2026-47876 VMXNET3 VM-escape, CVE-2026-41703 out-of-bounds read, CVE-2026-41709 insufficient ESX logging) only to the extent needed for accurate scoping of the single advisory, since all five ship in the same VMSA and the same patch trains.

Key findings

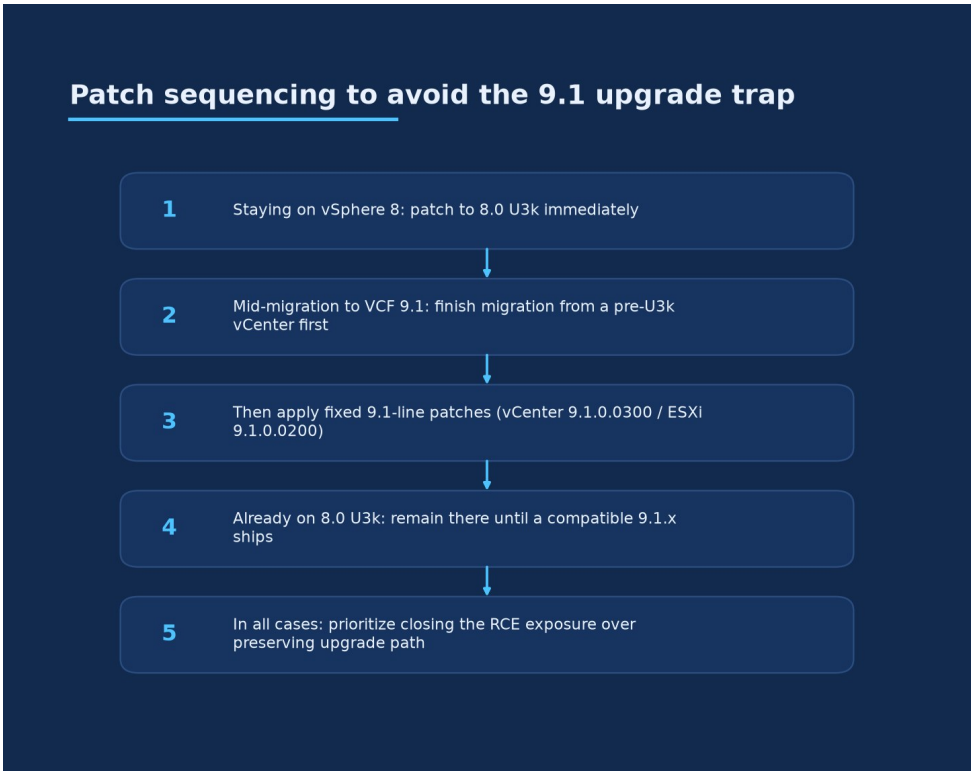


Disclosure timeline (2026) - Source: Ask Anything analysis - generated from the report's cited data

- CVE-2026-59309 is an authentication bypass in the VMware Directory Service (vmdir) affecting vCenter Server; CVSSv3.1 9.8, vector AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, CWE-303. [strong - vendor and NVD confirmed]
- CVE-2026-59310 is a directory-traversal vulnerability (CWE-22) in the vCenter Syslog Server enabling arbitrary code execution; CVSSv3.1 9.8, identical vector to CVE-2026-59309. [strong - vendor and NVD confirmed]
- Both vulnerabilities are exploitable by an unauthenticated attacker with mere network access/reachability to the affected vCenter service - no credentials, no user interaction, no local access required. [strong]
- Broadcom states explicitly that there are no workarounds for either CVE-2026-59309 or CVE-2026-59310; vendor patching is the only remediation path. [strong - direct vendor statement]
- Fixed versions: vCenter Server 8.0 Update 3k (build 25600417), VMware Cloud Foundation/vSphere Foundation 9.0.2.0100, and VMware Cloud Foundation/vSphere Foundation 9.1.0.0300. [strong]

- Broadcom has not disclosed the specific vulnerable endpoint, protocol operation, token/parsing defect, or exact bypass condition for either CVE; independent researchers confirm the public description is "intentionally limited." [strong - confirmed by direct quotation of advisory language]
- Broadcom and Rapid7 both report no evidence of in-the-wild exploitation and no known public proof-of-concept exploit code as of July 30-31, 2026. [strong, but time-perishable - status can change within days]
- Claims that CVE-2026-59309 was added to CISA's KEV catalog on July 27, 2026 predate the advisory's own July 29, 2026 publication date and could not be corroborated against CISA's catalog directly; treat as unverified/likely erroneous. [unproven]
- vCenter Server has been added to CISA's KEV catalog ten separate times historically for prior vulnerabilities, per Rapid7 - a strong base-rate signal that unauthenticated, network-reachable vCenter bugs convert to active exploitation with above-average frequency once technical details leak. [moderate - historical base rate, not a specific prediction for these two CVEs]
- Upgrading a vCenter 8.0 deployment to Update 3k blocks the subsequent in-place upgrade path to VMware Cloud Foundation/vSphere Foundation 9.1.0 or 9.1.0-based patches, per Broadcom's own release notes - a "back-in-time" restriction that requires migration sequencing decisions. [strong - vendor-documented]
- Three additional CVEs ship in the same advisory: CVE-2026-47876 (CVSS 9.3, VMXNET3 out-of-bounds write enabling guest-to-host VM escape, credited to Nguyen Hoang Thach of STARLabs SG via Trend Micro Pwn2Own), CVE-2026-41703 (CVSS up to 7.6, out-of-bounds read/information disclosure/DoS across ESX, Workstation, Fusion, credited to Maxim Suhanov), and CVE-2026-41709 (CVSS 2.7, insufficient ESX administrative logging, credited to CrowdStrike). [strong]
- CVE-2026-59309 and CVE-2026-59310 are credited to Atredis Partners; Broadcom's advisory language does not describe them as a chained attack, and independent analysis explicitly cautions defenders against assuming one vulnerability is a prerequisite for the other absent vendor confirmation. [strong on attribution; moderate/cautionary on the "not chained" characterization, since Broadcom has not ruled a chain in or out]
- Rapid7 shipped unauthenticated version-detection checks in InsightVM, Nexpose, and Exposure Command by July 30, 2026; Qualys published QIDs 388184, 216356, and 216358 the same day - both are presence/version checks, not exploit-attempt detections, because no public exploit signature exists yet. [strong]
- No CVSS-vector-level or NVD-published detail distinguishes a network port, API path, or log-ingestion protocol for either flaw; all currently circulating "likely LDAP port 389" or "likely syslog UDP/514" style claims are analyst inference, not vendor confirmation. [unproven - flagged explicitly by independent technical review]

Why this advisory matters operationally



Patch sequencing to avoid the 9.1 upgrade trap - Source: Ask Anything analysis - generated from the report's cited data

vCenter Server is the single pane of glass that manages authentication, role-based access control, inventory, templates, distributed resource scheduling, and orchestration for an entire vSphere estate. A successful authentication bypass against vmdir does not compromise one virtual machine - it compromises the identity and authorization plane governing every ESXi host, VM, datastore, and snapshot the appliance manages. Historically, unauthenticated RCE-class vCenter vulnerabilities (e.g., the 2021 vCenter vSAN plugin flaw CVE-2021-21985 and the 2023 DCERPC heap overflow CVE-2023-34048) have been weaponized by ransomware affiliates and state-linked actors specifically because compromising vCenter provides a single foothold from which to stage mass encryption of hosted VMs or exfiltrate data across an entire virtualization cluster. Rapid7's observation that vCenter has been added to CISA's KEV catalog ten separate times is the empirical basis for treating "no known exploitation yet" as a temporary state rather than a durable one (Rapid7, 2026).

CVE-2026-59309 - vCenter authentication bypass (VMware Directory Service)

Component: VMware Directory Service (vmdir), the embedded LDAP directory service that backs vCenter Single Sign-On (SSO), stores SSO users/groups, solution-user certificates, and password policies for the Platform Services Controller functionality now embedded in the vCenter Server Appliance.

Vendor description (verbatim): "VMware vCenter contains an authentication bypass vulnerability in the VMware Directory Service. A malicious actor with network access to vCenter may exploit this issue to bypass authentication and gain unauthorized access to the system" (Broadcom Support Portal VMSA-2026-0006, 2026; mirrored verbatim in NVD CVE-2026-59309, 2026).

Scoring: CVSSv3.1 base score 9.8/Critical. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H. CWE-303: Incorrect Implementation of an Authentication Algorithm (NVD CVE-2026-59309, 2026).

What is and is not known about mechanism: Every primary and secondary source reviewed for this report converges on the same limitation: Broadcom's public advisory text does not identify the specific vmdir operation, LDAP bind path, token type, SAML/OIDC assertion handling defect, or session-establishment logic responsible for the bypass. An independent technical breakdown states this explicitly: "The public description is intentionally limited. Broadcom has not disclosed the vulnerable request, endpoint, protocol operation, token format, parsing defect, or exact condition that causes authentication to be bypassed" (Penligent Hacking Labs, 2026). CWE-303 as a classification is broad - it covers everything from token/signature verification errors to session-fixation-style logic flaws to trust-boundary mistakes in federated authentication handoffs - and does not by itself narrow the mechanism.

Implication for defenders: Do not build detection logic around an assumed attack surface (e.g., "block LDAP on TCP 389/636 and you're covered") without vendor confirmation, since vmdir is reachable through multiple internal channels (VMware endpoint certificate store service, the STS/SSO web endpoints on 443, and internal RPC between vCenter services) and the disclosed CWE does not specify which channel is defective. Analysts explicitly warn against speculative narratives such as assuming "an LDAP bypass on port 389," because acting on an unconfirmed assumption (e.g., blocking only 389/tcp) could produce false confidence while the actual vulnerable path remains open (Penligent Hacking Labs, 2026).

CVE-2026-59310 - vCenter Syslog Server directory traversal / RCE

Component: The vCenter Syslog Server - the built-in service that ingests syslog messages (typically forwarded from ESXi hosts and other infrastructure) into the vCenter Server Appliance's log-management subsystem.

Vendor description (verbatim): "VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code" (Broadcom Support Portal VMSA-2026-0006, 2026; NVD CVE-2026-59310, 2026).

Scoring: CVSSv3.1 base score 9.8/Critical. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - identical to CVE-2026-59309. CWE-22: Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") (NVD CVE-2026-59310, 2026).

Technical shape of the bug class (from CWE classification, not vendor mechanism disclosure): CWE-22 path-traversal vulnerabilities in log-ingestion services typically arise when a service accepts an attacker-influenced filename, hostname, or path component (for example, embedded in a syslog message's tag/hostname field, or in a configuration parameter controlling where per-source log files are written) and fails to canonicalize or restrict that value before using it in a filesystem write or file-inclusion operation. The consequence described by Broadcom - "execute arbitrary code" rather than merely "read arbitrary files" - indicates the traversal is being used for a write primitive (e.g., writing a web-accessible file, a scheduled task, a service configuration file, or a script the appliance

later executes) rather than a pure information-disclosure read. This is consistent with, but not confirmed to be identical to, the class of directory-traversal-to-RCE bugs seen historically in other log-management and file-upload services. This paragraph is CWE-class inference for defensive planning purposes, not a vendor-confirmed exploitation chain - Broadcom has not published exploitation mechanics for CVE-2026-59310.

Relationship to CVE-2026-59309: Multiple outlets covering the advisory describe the two vCenter CVEs side by side because they ship in the same patch and share the same CVSS score, but independent technical analysis explicitly cautions that Broadcom "has not published a combined attack sequence in which the authentication bypass enables the syslog flaw or the syslog flaw enables the authentication bypass" - treat them as two independent unauthenticated entry points into vCenter rather than a confirmed two-stage chain, while still patching both immediately (Penligent Hacking Labs, 2026).

The other three CVEs in VMSA-2026-0006 (scoping context)

Because VMSA-2026-0006 ships as one advisory covering five CVEs across multiple products with overlapping fixed-version trains, defenders patching the two critical vCenter issues will almost always be patching the other three simultaneously. Brief technical scoping:

- CVE-2026-47876 (CVSS 9.3, ESX/ESXi) - an out-of-bounds write in the VMXNET3 virtual network adapter. This is a guest-to-host VM escape: an attacker who already holds local administrative privileges inside a guest VM configured with a VMXNET3 adapter can leverage the flaw to execute code on the underlying ESX host. Credited to Nguyen Hoang Thach of STARLabs SG, discovered via Trend Micro's Pwn2Own competition (Broadcom Support Portal, 2026). This is a different threat model from the two vCenter CVEs - it requires an existing VM compromise with admin/root rights as a precondition - but it is severe because it breaks the hypervisor isolation boundary that most cloud and shared-hosting security models depend on.

- CVE-2026-41703 (CVSS 7.6 on ESX; 2.7 on Workstation/Fusion) - an out-of-bounds read causing information disclosure or denial-of-service. Credited to Maxim Suhanov. Affects ESX, Workstation, and Fusion (Broadcom Support Portal, 2026).

- CVE-2026-41709 (CVSS 2.7, ESX) - insufficient logging that allows an ESX administrator to perform certain operations without those actions being recorded, an integrity-of-audit-trail issue rather than a remote-exploitation issue. Credited to CrowdStrike (Broadcom Support Portal, 2026).

NSX, vCenter Operations, and vCenter Automation products are explicitly not affected by this advisory (Field Effect, 2026).

Full affected and fixed version matrix

Version data below is consolidated from Broadcom's advisory, Broadcom's techdocs release notes for vCenter 8.0 U3k, and the Canadian Centre for Cyber Security's mirrored advisory AV26-763, cross-checked against Qualys and Rapid7 summaries. Where a source characterized a version range imprecisely, the more specific vendor-originated figure is used.

| Product line | Affected versions | Fixed version | CVEs remediated |

|---|---|---|---|

| VMware vCenter Server | 8.0.x (prior to 8.0 U3k) | 8.0 Update 3k (build 25600417) | CVE-2026-59309, CVE-2026-59310 |

| VMware Cloud Foundation / vSphere Foundation | 9.0.x.x (prior to fix) | 9.0.2.0100 | CVE-2026-59309, CVE-2026-59310 |

| VMware Cloud Foundation / vSphere Foundation | 9.1.x.x (prior to fix) | 9.1.0.0300 | CVE-2026-59309, CVE-2026-59310 |

| VMware Cloud Foundation | 5.x (async-patched deployments) | Async patch to 8.0 U3k content / 5.2.x line | CVE-2026-59309, CVE-2026-59310 (via embedded vCenter) |

| VMware ESX/ESXi | 9.1.x.x | ESXi-9.1.0.0200 | CVE-2026-47876, CVE-2026-41703 |

| VMware ESX/ESXi | 9.0.x.x | 9.0.2.0100 | CVE-2026-47876, CVE-2026-41703 |

| VMware ESX/ESXi | 8.0.x | ESXi80U3k | CVE-2026-47876, CVE-2026-41703 |

| VMware Workstation | 25H2 and prior | 26H1 | CVE-2026-41703 |

| VMware Fusion | 25H2 and prior | 26H1 | CVE-2026-41703 |

| VMware Telco Cloud Platform | 3.0, 4.x, 5.0.x, 5.1.x | Per Broadcom response matrix (consult VMSA directly) | CVE-2026-59309, CVE-2026-59310 (via embedded vCenter) |

| VMware Telco Cloud Infrastructure | 3.0 | Per Broadcom response matrix (consult VMSA directly) | CVE-2026-59309, CVE-2026-59310 (via embedded vCenter) |

Sources: Broadcom Support Portal VMSA-2026-0006 (2026); Broadcom techdocs vCenter 8.0 U3k release notes (2026); Canadian Centre for Cyber Security AV26-763 (2026); Qualys ThreatPROTECT (2026); York University UIT bulletin (2026).

Caveat on Telco Cloud Platform/Infrastructure and Cloud Foundation 5.x line items: multiple secondary sources reference these product lines as in-scope but do not consistently publish exact per-version fixed builds in the excerpts available to this report; Broadcom's own advisory (linked in Sources) is the authoritative reference and should be consulted directly by any organization running Telco Cloud Platform/Infrastructure or VCF 5.x before relying on this table for a patch decision.

Build/package detail confirmed for the headline vCenter fix: vCenter Server Appliance 8.0 Update 3k - build 25600417, released July 29, 2026, packaged as VMware-vCenter-Server-Appliance-8.0.3.01000-25600417-patch-FP.iso (SHA256: a74f93a8a4e50dabbbc8db8c64767cd9a8647c78c56003b541a41d4984728ba4), download-gated behind Broadcom Support Portal authentication (Broadcom techdocs, 2026).

The upgrade-path trap: Broadcom's release notes state explicitly that "Upgrade from vCenter 8.0 Update 3k to vCenter 9.1.0 or any patch based on 9.1.0 is not supported" (Broadcom techdocs, 2026). Independent analysis characterizes this as a "back-in-time upgrade restriction": 8.0 U3k contains security fixes and code changes that are not yet present in the currently shipping 9.1.0 baseline, so installing 9.1.0 over a patched 8.0 U3k instance would silently regress those fixes, which Broadcom's supported-upgrade policy disallows (AngrySysops, 2026). Concretely, this means:

- Organizations planning to stay on vSphere 8 for the foreseeable future should patch to 8.0 U3k immediately with no reservations.

- Organizations actively mid-migration to VMware Cloud Foundation 9.1 should complete that upgrade first from a pre-8.0-U3k vCenter instance, then apply the fixed 9.1.0-line patches (vCenter 9.1.0.0300 / ESXi 9.1.0.0200) once on the 9.1 baseline - reversing this order strands the environment.

- Organizations already on 8.0 U3k should remain on that branch until Broadcom ships a 9.1.x release compatible with the U3k security baseline; there is no published timeline for that compatible release as of this report.

- In every scenario, Broadcom's and independent guidance is unanimous that closing the unauthenticated-RCE-class exposure takes priority over preserving a future upgrade path (AngrySysops, 2026; Broadcom Support Portal, 2026).

Exploitation status and public exploit code

As of the most recent data available for this report (July 30-31, 2026, roughly 48-72 hours post-disclosure):

- No confirmed in-the-wild exploitation. Broadcom's advisory and Rapid7's independent emerging-threat response both state there is no known evidence of exploitation or of active scanning/probing traffic targeting either CVE (Rapid7, 2026; BleepingComputer, 2026).

- No public proof-of-concept exploit code. Searches of major public PoC aggregation repositories (community-curated CVE PoC collections on GitHub, PocOrExp_in_Github tracking lists, and vendor/researcher blogs) returned no working exploit code for CVE-2026-59309 or CVE-2026-59310 as of this report's research window. This is consistent with Broadcom's own decision to withhold exploitation mechanics from the public advisory.

- CISA KEV status is unconfirmed and a specific claim about it appears erroneous. One secondary aggregator surfaced a claim that CVE-2026-59309 was "added to CISA's KEV catalog on July 27, 2026" - two days before Broadcom's own July 29, 2026 advisory publication date. That sequencing is implausible (KEV entries require a published CVE and, per CISA's own KEV inclusion criteria, evidence of active exploitation) and could not be independently corroborated against CISA's KEV catalog page directly during this research. NVD's own CISA-ADP (Authorized Data Publisher) supplemental entry for CVE-2026-59309, by contrast, records an SSVC (Stakeholder-Specific Vulnerability Categorization) assessment with the exploitation status field set to "none" as of July 30, 2026 (NVD CVE-2026-59309, 2026). Defenders should treat the July 27 KEV-addition claim as unverified/likely erroneous rather than plan around it, and should check CISA's KEV catalog directly for the current, authoritative status rather than relying on this report's snapshot, since KEV status is one of the fastest-changing facts in this entire dossier.

- Historical base rate argues for urgency regardless of current PoC status. Rapid7's framing - that vCenter Server has been added to the KEV catalog ten separate times historically - is the strongest available signal for how this specific disclosure is likely to evolve. Unauthenticated, network-reachable, CVSS 9.8 vCenter vulnerabilities have consistently attracted patch-diffing and weaponization by both

criminal ransomware affiliates and state-linked intrusion sets within a window that has historically ranged from days to a few weeks post-disclosure (Rapid7, 2026). The absence of a PoC on July 31, 2026 is not evidence the vulnerability is hard to exploit; it may simply reflect that reverse-engineering the vCenter 8.0 U3k / 9.0.2.0100 / 9.1.0.0300 patch diffs is still in progress across the security research and threat-actor community.

- No CVSS temporal score has been published by NVD or Broadcom incorporating exploit-code-maturity or remediation-level metrics as of this report; only the base score is currently available.

Detection guidance

Because the vulnerable request, endpoint, or parsing defect has not been disclosed, no vendor-published exploitation signature currently exists for either CVE. Detection posture accordingly splits into two tiers: presence/version detection (mature and available now) and behavioral/anomaly detection (the only option pending a disclosed IOC).

Tier 1 - Vulnerability presence detection (version fingerprinting):

- Rapid7 shipped unauthenticated vulnerability checks for CVE-2026-59309 and CVE-2026-59310 in InsightVM, Nexpose, and Exposure Command as of July 30, 2026 (Rapid7, 2026).

- Qualys published detection QIDs 388184, 216356, and 216358 covering the VMSA-2026-0006 product set in Qualys VMDR/ThreatPROTECT as of July 30, 2026 (Qualys ThreatPROTECT, 2026).

- Both of the above detect vulnerable version strings, not active exploitation attempts - treat a "vulnerable" finding as an inventory/patch-prioritization signal, not an incident.

- Baseline inventory action: enumerate every vCenter Server Appliance, embedded vCenter instance inside VMware Cloud Foundation/vSphere Foundation deployments, and any Telco Cloud Platform/Infrastructure deployment that embeds vCenter, and record its exact build number against the fixed-version matrix above. Do not rely on "vSphere 8" or "VCF 9" as sufficient version granularity - the difference between 8.0 U3j and 8.0 U3k is the entire security boundary here.

Tier 2 - Behavioral detection (pending disclosed IOCs), synthesized from independent technical guidance (Penligent Hacking Labs, 2026):

- Authentication/authorization correlation: Monitor for administrative or privileged vCenter sessions that do not have a corresponding successful authentication event in your identity provider (AD FS, Okta, Ping, or whichever IdP federates into vCenter SSO) or that lack an expected MFA challenge-response pair. An authenticated session without a matching upstream authentication event is the closest available proxy for an auth-bypass exploitation attempt.

- vmdir-specific log review: Review VMware Directory Service logs (/var/log/vmware/vmdird/vmdird-syslog.log on the vCenter Server Appliance, and the vmdir component logs bundled in a vc-support log bundle) for connection anomalies, unexpected bind attempts, and TLS/SSL negotiation errors around the disclosure window and going forward. Because the exact defect is undisclosed, look for anomalies relative to your own baseline (unusual source IPs, unusual bind DN patterns, error bursts) rather than a known-bad signature.

- SSO identity-store integrity checks: Periodically diff the SSO users, groups, and group-membership lists (particularts administrators/Administrators@vsphere.local group) against a known-good baseline. An authentication-bypass exploit that pivots into persistence would very plausibly create or modify SSO principals.

- Syslog service exposure and traffic review: Confirm whether the vCenter Syslog Server service is enabled and internet- or broadly-network-reachable at all; if it is receiving forwarded logs only from a tightly scoped set of ESXi hosts and management systems, restrict inbound reachability to exactly that set and monitor for any syslog traffic arriving from outside that expected source set - an out-of-scope source sending syslog traffic is the most plausible external signal of directory-traversal probing, even without a disclosed payload signature.

- Retrospective flow-log preservation: Because the traversal/bypass mechanism may be discovered and retroactively signatured by researchers in coming weeks, preserve NetFlow/firewall session logs showing any inbound connection to vCenter management-plane IP addresses and ports covering the weeks before and after July 29, 2026, so a retrospective hunt is possible once IOCs are published.

- Explicit anti-pattern: Do not accept "the session shows as authenticated" as proof of legitimate authentication. Independent guidance frames this directly: "An authentication result must not be accepted merely because a requester labels it as authenticated" (Penligent Hacking Labs, 2026) - build detections and access reviews around independently corroborated identity evidence, not vCenter's own session state, until the bypass mechanism is understood.

- Post-patch monitoring: After patching, watch for service crashes or restarts in the vmdir and syslog server processes, and for VMXNET3-related guest/host instability if also remediating CVE-2026-47876, as either could indicate a failed exploitation attempt against the pre-patch state or an unrelated patch-application issue worth investigating (Vulert, 2026).

Interim mitigations for teams that cannot patch immediately

Broadcom is unambiguous that there is no vendor-sanctioned workaround for CVE-2026-59309 or CVE-2026-59310 (Broadcom Support Portal, 2026; and confirmed in the VMSA's own FAQ, which states: "There may be other mitigations and compensating controls available in your organization, depending on your security posture, defense-in-depth strategies, and configurations of perimeter firewalls and appliance firewalls," explicitly stopping short of endorsing any specific compensating control as sufficient - GitHub vcf-security-and-compliance-guidelines VMSA-2026-0006 FAQ, 2026). Treat every item below as risk reduction, not risk elimination - none of them close the vulnerabilities, and all should be paired with an aggressive patch timeline.

- Network isolation of the vCenter management interface. Restrict TCP/443 (and any other vCenter management port) reachability to a dedicated, tightly access-controlled management subnet or VLAN. Since both CVEs require only network reachability and no credentials, reducing the population of hosts/users that can route to vCenter at all is the single highest-leverage compensating control available.

- Mandatory jump-host/bastion access. Require all administrative access to vCenter to transit a

hardened jump host rather than direct routing from end-user or general-server subnets, so that any exploitation attempt must first compromise the bastion, adding a detectable, loggable hop.

- Phishing-resistant MFA on every remote path into the management plane (jump host login, VPN, any web console proxy in front of vCenter) - this does not stop the vCenter-side authentication bypass itself, but reduces the odds that credential-based lateral movement compounds the exposure while unpatched.

- Restrict or disable unnecessary reachability to the Syslog Server component specifically. If the vCenter Syslog Server is not required to be reachable from outside a known, small set of ESXi hosts and log-forwarding systems, scope its firewall rules to exactly that set, and disable the service entirely on any vCenter instance that does not actively use it for centralized log collection, pending confirmation from Broadcom on the precise mitigation value of this step for CVE-2026-59310.

- Increase logging verbosity and shorten the session/log review cadence. Move to daily (not weekly) review of vCenter SSO administrative session activity and vmdir logs until patched, given the absence of a disclosed exploitation signature - increased human review frequency is a partial substitute for the automated detection that isn't yet possible.

- Segment and snapshot-isolate the vCenter Server Appliance itself so that, in the event of compromise, the blast radius of an attacker who obtains vCenter-level access is constrained from directly reaching every ESXi host's management interface without an additional hop or credential.

- Accelerate patch testing rather than patch timeline. Because there is no workaround, the operationally correct read of "interim mitigation" here is: compress the validation/change-control cycle for the vCenter 8.0 U3k / 9.0.2.0100 / 9.1.0.0300 patch as much as your change-management process allows, rather than treating compensating controls as a durable substitute for patching. Broadcom explicitly frames this as an emergency change warranting expedited handling, including acceptance of the vCenter service interruption the update entails (Broadcom Support Portal, 2026; Field Effect, 2026).

- If running VMware Cloud Foundation 5.x or Telco Cloud Platform/Infrastructure, confirm the exact async-patch or fixed-version guidance directly against Broadcom's advisory before assuming the standalone vCenter 8.0 U3k build applies unmodified to your deployment topology, since these product lines consume vCenter as an embedded component with their own release trains.

None of items 1-7 substitute for patching. They exist to reduce dwell-time risk for organizations that have a legitimate, time-boxed operational reason (change-freeze windows, validation requirements, the VCF 9.1 upgrade-sequencing conflict described above) for not patching within the first days after disclosure.

Open questions

- Exact vulnerable request/endpoint for CVE-2026-59309. Broadcom has not disclosed which vmdir-facing interface (LDAP bind path, STS/SSO web endpoint, internal RPC channel, or a specific token/assertion validation routine) contains the defect. Until this is published or independently reverse-engineered and confirmed, all "which port to block" guidance is inference, not fact.

- Exact traversal primitive and code-execution mechanism for CVE-2026-59310. It is not publicly confirmed whether the "arbitrary code execution" outcome is achieved via writing an executable/interpretable file to a web-accessible or scheduled-task path, via overwriting an existing configuration/service file, or via some other primitive. This materially affects what a targeted YARA rule, EDR detection, or WAF rule would need to match.

- Whether the two vCenter CVEs are chainable. No vendor-confirmed attack sequence links CVE-2026-59309 and CVE-2026-59310; independent analysis explicitly declines to assume a chain in either direction. Whether a real-world intrusion would use them together (e.g., traversal-write to obtain code execution, followed or preceded by an independent auth bypass) is unresolved.

- True CISA KEV status. As discussed above, a specific "added July 27, 2026" claim for CVE-2026-59309 appears to predate the advisory and could not be corroborated; the authoritative, current KEV status should be checked directly against CISA's catalog rather than taken from this report.

- Time-to-weaponization. Given the ten-times KEV history for vCenter Server generally, whether these two specific CVEs will be reverse-engineered into a working exploit in days versus weeks is unknown; the withheld technical detail may modestly slow that process relative to advisories that ship more implementation detail, but does not prevent it, since patch-diffing against the 8.0 U3k / 9.0.2.0100 / 9.1.0.0300 binaries remains available to any sufficiently resourced researcher or threat actor.

- Full Telco Cloud Platform/Infrastructure and VMware Cloud Foundation 5.x version-matrix precision. Secondary sources are inconsistent on exact fixed builds for these product lines; only Broadcom's own advisory (linked in Sources) should be treated as authoritative, and this report could not fully reconcile all cited version strings for these specific product lines across sources.

- Whether a compatible VMware Cloud Foundation 9.1.x release resolving the "back-in-time" upgrade block will ship, and when. No timeline has been published as of this report.

Practical synthesis

Who this applies to: Any organization running a self-managed vCenter Server Appliance (standalone vSphere 8.0.x, or embedded within VMware Cloud Foundation/vSphere Foundation 9.0.x/9.1.x, VMware Cloud Foundation 5.x, or VMware Telco Cloud Platform/Infrastructure) with the management interface reachable - even only internally - from any network segment not under the same trust level as the vCenter appliance itself. Given the vulnerabilities require only network reachability and no credentials, "internal-only" reachability is not a mitigating factor by itself unless the internal network segment reaching vCenter is itself tightly access-controlled.

Decision framework:

- Inventory first. Identify every vCenter instance (standalone and embedded) and its exact build number against the version matrix above. Do this before anything else - you cannot correctly sequence patch-vs-upgrade decisions without knowing your starting point.

- If not mid-migration to VCF 9.1: patch to 8.0 U3k (or the appropriate 9.0.2.0100/9.1.0.0300 build if already on those trains) as an emergency change, with normal validation compressed rather than

skipped.

- If actively mid-migration to VCF 9.1: complete the 9.1 upgrade first from the pre-patch vCenter baseline, then apply the fixed 9.1.0.0300/ESXi 9.1.0.0200 patches immediately after - do not patch to 8.0 U3k first, or the upgrade path will be blocked per Broadcom's own release notes.

- While patch validation is in flight (hours to low single-digit days, not weeks): apply the network-isolation, jump-host, MFA, and logging-cadence compensating controls above, understanding they reduce but do not eliminate risk.

- Deploy Tier 1 (version) detection immediately via whatever vulnerability management platform you run (Rapid7 InsightVM/Nexpose/Exposure Command or Qualys VMDR, at minimum) to get an accurate, continuously-refreshed inventory of exposure - do not rely on a one-time manual inventory pass given how frequently vCenter patch trains are updated.

- Stand up Tier 2 (behavioral) monitoring now, not after an incident. The absence of a disclosed IOC means the behavioral baseline (expected SSO session patterns, expected syslog source IPs, expected vmdir log volume) is only useful if you started collecting it before an intrusion, not after.

- Re-check exploitation and KEV status on a recurring (at minimum daily, ideally continuous feed-driven) basis for the first several weeks post-disclosure, given the historical base rate of vCenter vulnerabilities converting to active exploitation.

What to measure going forward: patch compliance rate across all vCenter instances (standalone + embedded) against the fixed-version matrix, mean time from disclosure to patch for this specific advisory versus your organization's historical vCenter patch SLA, count of administrative vCenter sessions per day lacking a corroborating IdP authentication event, and syslog-server inbound source-IP drift versus baseline.

Evidence & caveats

Established (vendor- and NVD-confirmed): the existence, CVSS scores, CVSS vectors, CWE classifications, affected component names (vmdir for CVE-2026-59309, syslog server for CVE-2026-59310), and fixed version numbers for the headline vCenter builds (8.0 U3k, 9.0.2.0100, 9.1.0.0300).

Established but time-perishable: "no known exploitation" and "no known public PoC" - both are point-in-time facts as of roughly July 30-31, 2026 and should be re-verified before this report is relied upon at any later date.

Disputed/unverified: the specific claim that CVE-2026-59309 was added to CISA's KEV catalog on July 27, 2026. This predates the advisory's own publication and could not be corroborated against CISA's catalog directly during this research; NVD's own CISA-ADP SSVC supplement instead records an exploitation status of "none" as of July 30, 2026.

Preliminary/inference, not vendor-confirmed: any characterization of CVE-2026-59310's traversal-to-RCE mechanism as a "write primitive" is CWE-class-informed inference by this report's authors for defensive-planning purposes, not a Broadcom-confirmed technical detail. Similarly, any statement about which specific network port or protocol is involved in either vulnerability is explicitly

not vendor-confirmed and is flagged as such by independent technical analysts as well.

Missing/not yet available: the exact vulnerable code path for either CVE; a CVSS temporal score incorporating exploit-code-maturity or remediation-level metrics; precise fixed-version strings for VMware Telco Cloud Platform/Infrastructure and VMware Cloud Foundation 5.x deployments (defer to Broadcom's own advisory for these); any public exploit code, detection signature, or YARA/Sigma rule tied specifically to these two CVEs; and any confirmed real-world exploitation case study, since none has been reported as of this writing.

Not generalizable: the ten-times CISA KEV historical statistic for vCenter Server is a base rate across many prior, technically distinct vulnerabilities over multiple years - it is directional evidence for urgency, not a specific probability estimate for CVE-2026-59309 or CVE-2026-59310 individually.

Sources

[1] VMSA-2026-0006 - Broadcom Support Portal Security Advisory (2026) -- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

[2] VMSA-2026-0006 FAQ/Q&A - vmware/vcf-security-and-compliance-guidelines (GitHub) (2026) -- https://github.com/vmware/vcf-security-and-compliance-guidelines/tree/main/security-advisories/vmsa-2026-0006

[3] NVD - CVE-2026-59309 Detail -- https://nvd.nist.gov/vuln/detail/CVE-2026-59309

[4] NVD - CVE-2026-59310 Detail -- https://nvd.nist.gov/vuln/detail/CVE-2026-59310

[5] VMware vCenter Server 8.0 Update 3k Release Notes - Broadcom TechDocs (2026) -- https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/release-notes/vcenter-server-update-and-patch-release-notes/vsphere-vcenter-server-80u3k-release-notes.html

[6] "Critical VMware vCenter Vulnerabilities Allow Authentication Bypass and Remote Code Execution (CVE-2026-59309, CVE-2026-59310)" - Rapid7 Blog (2026) -- https://www.rapid7.com/blog/post/etr-critical-vmware-vcenter-vulnerabilities-allow-authentication-bypass-and-remote-code-execution-cve-2026-59309-cve-2026-59310/

[7] "Three Critical VMware Flaws Allow Auth Bypass, Code Execution, and VM Escape" - The Hacker News (2026) -- https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html

[8] "VMware fixes three critical flaws allowing auth bypass, VM escapes" - BleepingComputer (2026) -- https://www.bleepingcomputer.com/news/security/vmware-fixes-three-critical-flaws-allowing-auth-bypass-vm-escapes/

[9] "VMware ESX, vCenter, Workstation, and Fusion Multiple Vulnerabilities" - Qualys ThreatPROTECT (2026) -- https://threatprotect.qualys.com/2026/07/30/vmware-esx-vcenter-workstation-and-fusion-multiple-vulnerabilities/

[10] "CVE-2026-59309: VMware vCenter Authentication Bypass and Management Plane Risk" - Penligent Hacking Labs (2026) -- https://www.penligent.ai/hackinglabs/cve-2026-59309/

[11] "vSphere 8.0 Update 3k Fixes Critical CVEs - but Temporarily Blocks the VCF 9.1 Upgrade Path" - AngrySysOps (2026) -- https://angrysysops.com/2026/07/30/vsphere-8-0-update-3k-fixes-critical-cves-but-temporarily-blocks-the-vcf-9-1-upgrade-path/

[12] "Broadcom Patches Critical Vulnerabilities Affecting Multiple VMware Products" - Field Effect (2026) -- https://fieldeffect.com/blog/broadcom-patches-critical-vcenter-vulnerabilities

[13] "Critical VMware Flaws Allow Attackers to Bypass Authentication and Gain Access to the System" - Cyber Security News (2026) -- https://cybersecuritynews.com/vmware-flaws-allow-authentication-bypass/

[14] "Critical VMware vCenter Flaws Let Remote Attackers Bypass Authentication and Execute Code" - GBHackers (2026) -- https://gbhackers.com/critical-vmware-vcenter-flaws/

[15] "VMware vCenter Server multiple vulnerabilities (CVE-2026-59309, CVE-2026-59310)" - York University UIT Security Bulletin (2026) -- https://www.yorku.ca/uit/2026/07/vmware-vcenter-server-multiple-vulnerabilities-cve-2026-59309cve-2026-59310/

[16] "VMware security advisory (AV26-763)" - Canadian Centre for Cyber Security (2026) -- https://www.cyber.gc.ca/en/alerts-advisories/vmware-security-advisory-av26-763

[17] "Critical VMware Flaws: vCenter and VM Escape" - Vulert Blog (2026) -- https://vulert.com/blog/vmware-critical-flaws-vcenter-esxi-vm-escape/

[18] "Critical VMware vCenter Vulnerabilities Allow Authentication Bypass and Remote Code Execution (CVE-2026-59309, CVE-2026-59310)" - Noise/getoto.net (Rapid7 syndication) (2026) -- https://noise.getoto.net/2026/07/30/critical-vmware-vcenter-vulnerabilities-allow-authentication-bypass-and-remote-code-execution-cve-2026-59309-cve-2026-59310/

[19] "Broadcom Patches CVE-2026-59309 & CVE-2026-59310 (CVSS 9.8) in VMware" - SecurityOnline (2026) -- https://securityonline.info/vmware-authentication-bypass-cve-2026-59309/

[20] "VMSA-2026-0006: Broadcom Patches CVSS 9.8 vCenter Auth Bypass and RCE" - Falcon Internet Blog (2026) -- https://www.falconinternet.net/blog/vmsa-2026-0006-vcenter-auth-bypass-rce-broadcom-patches-july-2026

[21] "VMSA-2026-0006: Up to 3 VMware vulnerabilities are rated as 'Critical'" - IPSIP (2026) -- https://www.ipsip.vn/en/post/vmsa-2026-0006-up-to-3-vmware-vulnerabilities-are-rated-as-critical

[22] "Broadcom Patches Critical VMware ESXi Vulnerability Enabling Host Code Execution" - Security Affairs (2026) -- https://securityaffairs.com/196231/security/broadcom-patches-critical-vmware-esxi-vulnerability-enabling-host-code-execution.html