Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Suspected China-Nexus APT Weaponizes CVE-2026-59310

Date of Publication	Admiralty Code	TA Number
August 20, 2026	A1	TA2026241

Summary

First Seen: July 29, 2026
Threat Actor: Uncategorized Chinese-nexus intrusion set (suspected China-nexus APT, Chinese-speaking)
Malware: Babuk-derived ESXi ransomware (".babyk" extension)
Unique public victim IPs: 361
Affected Products: VMware vCenter Server, VMware Cloud Foundation, VMware vSphere Foundation, VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure
Targeted Countries: Germany, United States, Turkey, Iran, France, Brazil, India, Japan, Singapore, Australia, South Africa, Mexico, United Kingdom, Spain, Italy, Poland, Russia, South Korea, Canada, Netherlands, Belgium, Switzerland, Austria, Czechia, Sweden, Finland, Norway, Denmark, Ukraine, Romania, Greece, Bulgaria, Portugal, Israel, Pakistan, Bangladesh, Sri Lanka, Thailand, Vietnam, Malaysia, Indonesia, Taiwan, Hong Kong, Colombia, Peru, Argentina
Targeted Industries: Technology, Higher education, Research, Telecommunications
Impact: CVE-2026-59310 is a critical directory traversal flaw in the VMware vCenter Syslog server that allows an unauthenticated attacker with network access to write to /etc/cron.d and gain immediate root code execution on the appliance. Exploitation began five days after disclosure, and since then, it has tracked 361 victim IPs across 47 countries, concentrated in Germany, the US, Turkey, Iran, and France, and skewed toward technology, higher education, and telecommunications. The business impact of CVE-2026-59310 is severe because vCenter is the control plane for the entire virtual estate rather than a single application, so one unauthenticated remote code execution against it collapses the blast radius of the whole environment into a single point of failure.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-59310	Broadcom VMware vCenter Path Traversal Vulnerability	Broadcom VMware vCenter	✗	✓	✓
CVE-2026-59309	Broadcom VMware vCenter Authentication Bypass Vulnerability	Broadcom VMware vCenter	✗	✗	✓

Exploitation Timeline

Broadcom publishes VMSA-2026-0006 covering **CVE-2026-59310**

July 29, 2026

August 3, 2026

First **CVE-2026-59310** exploitation begins

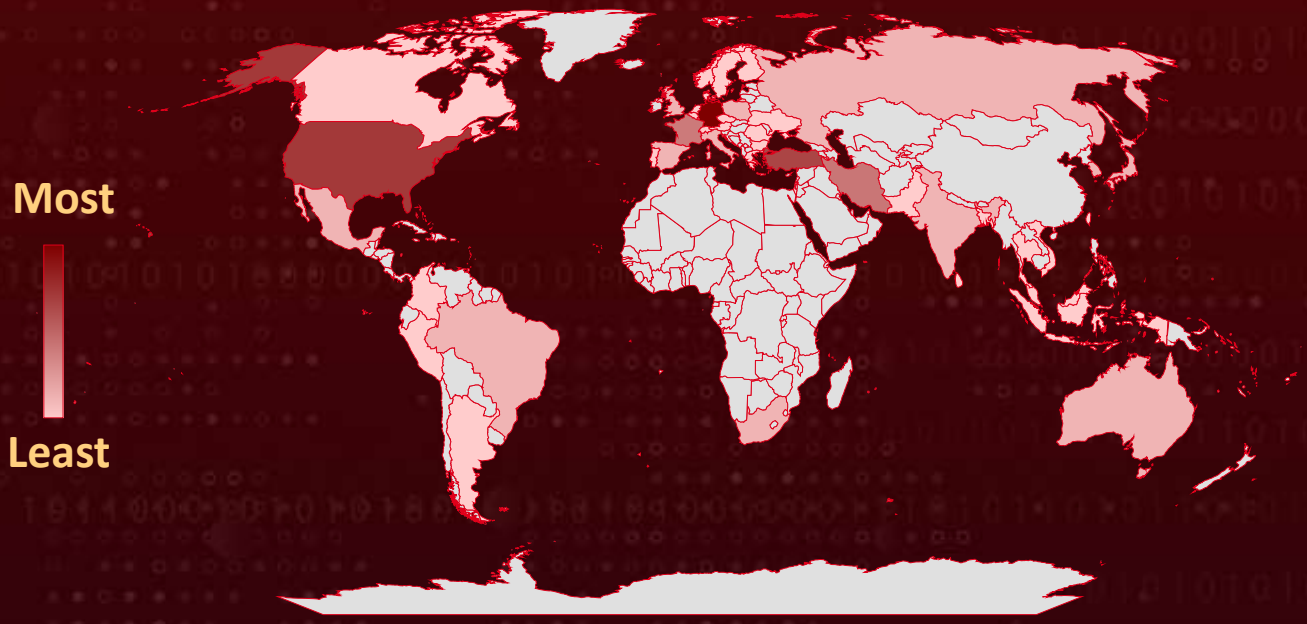
CVE-2026-59310 Campaign exploitation peaks, 151 new victims

August 4, 2026

August 7, 2026

Full victim population of **361 unique victim IPs across 47 countries** identified to date

Targeted Regions



Targeted Non-Targeted

Vulnerability Details

#1

CVE-2026-59310 is a critical directory traversal vulnerability in the VMware vCenter Syslog server that allows an attacker with network access to the appliance to execute arbitrary code, and it is being exploited at a global scale by a suspected China-nexus advanced persistent threat actor. Broadcom disclosed the flaw on July 29, 2026, in advisory VMSA-2026-0006 alongside CVE-2026-59309, an authentication bypass in the VMware Directory Service, and stated that no workaround exists. Both issues were privately reported to Broadcom, which reported no known exploitation at the time of publication.

#2

Exploitation nonetheless began five calendar days later. The first compromised systems connected to actor infrastructure on August 3, 2026, with the campaign expanding sharply on August 4 when 151 additional victim IP addresses appeared and reaching 343 of an eventual 361 unique victim IP addresses by August 5. Those 361 addresses span 47 countries, concentrated in Germany with 55, the United States with 41, Turkey with 38, Iran with 26, and France with 25, and cluster by sector in technology, software and cybersecurity, followed by higher education and research, and then telecommunications.

#3

The observed intrusion chain abuses the syslog path-handling behavior to write actor-controlled content into /etc/cron.d, giving the actor immediate non-interactive code execution as root on the vCenter Server Appliance without any prior authentication event. From there, the actor stages the linuxFile WebSocket backdoor and the open-source reverse_ssh framework from multiple actor-controlled and third-party hosting services, plants a JSP webshell inside the vCenter Perfcharts application, grants the perfcharts service account passwordless sudo, harvests the vCenter machine account credential from the vmdir registry hive, creates multiple vSphere SSO administrator accounts, and ultimately deploys Babuk-derived ransomware against ESXi hosts.

#4

With moderate confidence that the operator is a Chinese-speaking actor probably working in a UTC+8 environment, based on Simplified Chinese artifacts in attacker scripts, apparent reuse of research from a Chinese security publication, repeated use of Chinese-language tooling and management software, victimology that excludes mainland China, and activity patterns consistent with UTC+8 working hours, while noting that it has insufficient evidence to associate the campaign with a named Chinese threat group or to determine state direction.

#5

The root cause is insufficient constraints on pathnames handled by the vCenter Server Appliance syslog service, which allows relative traversal sequences supplied in log data to escape the configured syslog output directory. The recovered log entries preserve the exploit format, in which a traversal string of the form ../../../../etc/cron.d/zz-poc59310 appears embedded in a malformed syslog record accompanied by a crontab-formatted payload line and a fabricated timestamp dated to January 2026 that is inconsistent with the surrounding August 2026 entries.

#6

The effect is that actor-controlled content is written into a privileged execution location. Because the syslog service runs with sufficient privilege on the appliance, the resulting file is picked up and executed by the cron daemon in a root context, which converts what is nominally a file write primitive into unauthenticated remote code execution as root. This is the mechanism that distinguishes the flaw from an ordinary path traversal read: the traversal target is chosen so that an existing, trusted system service performs the execution on the attacker's behalf.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-59310	VMware vCenter (9.1.x.x, 9.0.x.x, 8.0, 7.0), VMware Cloud Foundation (9.1.x.x, 9.0.x.x, 5.x), VMware vSphere Foundation (9.1.x.x, 9.0.x.x), VMware Telco Cloud Platform (3.0, 4.x, 5.0.x, 5.1.x), VMware Telco Cloud Infrastructure (3.0)	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vsphere_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*:*:*	CWE-22
CVE-2026-59309			CWE-303

Recommendations

Patch vCenter Immediately: Apply the fixed release identified in the VMSA-2026-0006 response matrix for your deployment without delay, meaning vCenter 9.1.0.0300 for the 9.1 branch, 9.0.2.0100 for the 9.0 branch, and 8.0 U3k or 8.0 U2f for the 8.0 branch depending on which branch is deployed. VMware Cloud Foundation 5.x requires an asynchronous patch to vCenter 8.0 U3k, and Telco Cloud Platform and Telco Cloud Infrastructure deployments should follow KB449886. Broadcom states that no workaround exists for this vulnerability, so there is no configuration change that substitutes for the update. Organizations still running vCenter 7.0 have no generally available fix and should contact Broadcom Support if they hold an extended support contract, treating those appliances as high-priority candidates for isolation or accelerated migration in the interim.

Assume Compromise and Hunt Before Declaring Closure: Patching does not evict an actor who exploited the flaw before the update was applied, because persistence established through reverse_ssh, systemd services, cron jobs and SSH keys survives the upgrade. Any internet-exposed vCenter appliance that was unpatched at any point after July 29, 2026 should be treated as potentially compromised and subjected to forensic review rather than considered remediated. Prioritize inspection of /etc/cron.d for files carrying poc59310 or syslog.log naming patterns, cron entries impersonating VMware services with vmware-vpxd-stats, vmware-perf-collect or vmware-perf-sync prefixes, unexpected systemd units, the presence of /etc/sudoers.d/vmware-perf, and any file named vmware-perf-update.jsp under the Perfcharts statsreport web application directories. Note that the actor deliberately deleted scripts and cron jobs after use, so system logging may retain evidence of commands whose files are already gone.

Audit vSphere SSO and ESXi Accounts for Unauthorized Identities: The observed intrusion created multiple administrative identities through distinct mechanisms, including an SSO account named adminuser added to the built-in Administrators group, a second account named vcadmin created through a Base64-encoded Python script, a service-style account created by external LDAP Add operation against vmdir using a pre-existing administrative account the actor had taken over, and local adminuser accounts on individual ESXi hosts staged shortly before ransomware execution. Enumerate all vSphere SSO principals and all local ESXi accounts, validate each against your authorized inventory, remove anything unrecognized, and rotate credentials for legitimate administrative accounts because at least one existing privileged account was compromised in the observed case. Also review root authorized_keys files on vCenter for SSH public keys the actor may have added.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1588: Obtain Capabilities	T1588.002: Tool
	T1583: Acquire Infrastructure	T1583.004: Server
		T1583.006: Web Services
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1053: Scheduled Task/Job	T1053.003: Cron
	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
		T1059.006: Python
Persistence	T1543: Create or Modify System Process	T1543.002: Systemd Service
	T1053: Scheduled Task/Job	T1053.003: Cron
	T1505: Server Software Component	T1505.003: Web Shell
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1136: Create Account	T1136.002: Domain Account
		T1136.001: Local Account
	T1078: Valid Accounts	T1078.002: Domain Accounts
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.003: Sudo and Sudo Caching

Tactic	Technique	Sub-technique
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1070: Indicator Removal	T1070.004: File Deletion
	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
	T1497: Virtualization/Sandbox Evasion	
	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Credential Access	T1552: Unsecured Credentials	T1552.002: Credentials in Registry
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
Lateral Movement	T1021: Remote Services	T1021.004: SSH
Command and Control	T1105: Ingress Tool Transfer	
	T1219: Remote Access Software	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	
	T1102: Web Service	

Tactic	Technique	Sub-technique
Impact	T1489: Service Stop	
	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6687083075c0dfcd86d4e0f5541550e29987de5e729efd5687ab0db1cd116b2c
SHA1	e876ceb47ba092420a97724a957152b3808568b0
IPv4	5[.]34[.]176[.]100, 5[.]34[.]177[.]38, 78[.]135[.]91[.]204, 141[.]95[.]158[.]73, 146[.]56[.]116[.]119, 146[.]59[.]252[.]178, 185[.]144[.]28[.]120, 192[.]255[.]141[.]13
IPv4:Port	5[.]34[.]176[.]100[:]5244, 5[.]34[.]177[.]38[:]9564, 5[.]34[.]177[.]38[:]9861, 185[.]144[.]28[.]120[:]3232, 192[.]255[.]141[.]13[:]7788, 192[.]255[.]141[.]13[:]8080
Domains	intel[.]se9ly9upbhay[.]shop, se9ly9upbhay[.]shop, profound-beijinho-504b1f[.]netlify[.]app
URLs	hxxp[:]//5[.]34[.]177[.]38[:]9861/linuxFile, hxxp[:]//5[.]34[.]177[.]38[:]9564/linuxFile, hxxp[:]//185[.]144[.]28[.]120[:]3232/esxi[.]sh, hxxp[:]//185[.]144[.]28[.]120[:]3232/esxi_amd64, hxxps[:]//tmpfiles[.]org/dl/1785758754[.]8cc04603f0b76caa/wqwNICA6Rb9o/systemlog[.]txt, hxxps[:]//profound-beijinho-504b1f[.]netlify[.]app/f, ws[:]//intel[.]se9ly9upbhay[.]shop[:]8080/ws
Email	pikpak0066test[@]outlook[.]com

TYPE	VALUE
Hostname	kali[.]kali
Filename	linuxFile, systemlog, systemlog.txt, linux_x86, esxi.sh, esxi_amd64, backup, run.sh, _post_launch.sh, zz-poc59310, zz-poc59310-syslog.log, vmware-perf-update.jsp, sso_domain.txt, tmpclean
File Path	/etc/cron.d/zz-poc59310, /etc/cron.d/zz-poc59310-syslog.log, /etc/sudoers.d/vmware-perf, /tmp/linuxFile, /tmp/.x/, /tmp/.x/systemlog, /tmp.x/systemlog, /tmp/.x.py, /tmp/.a.ldif, /tmp/.ldap.out, /tmp/.ldappw, /tmp/.sso_domain, /tmp/.vmware-perf-upd.sh, /var/run/backup, /usr/local/bin/tmpclean, /root/.local/share/cg4nQW9TOxeq/, /usr/lib/vmware-perfcharts/tc-instance/webapps/statsreport/vmware-perf-update.jsp
User Agent	GoodMoodle-VCProbe/1.0, GoodMoodle-VCFleet/1.0
Service Name	sys-9436d8.service, network-manager
Account Name	adminuser, vcadmin, vcenter_admin, svc_dAi7dDGBKk
File Extension	.babyk

Patch Link

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

References

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

https://medium.com/@quirso_de/the-great-clean-up-job-337ccefd2bee

https://medium.com/@quirso_de/global-exploitation-of-cve-2026-59310-by-suspected-chinese-nexus-apt-related-cve-2026-59309-443a79e1466d

https://medium.com/@quirso_de/active-exploitation-of-cve-2026-59310-361-victim-ips-across-47-countries-9783187cc6ff

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

August 20, 2026 • 09:00 AM

More at www.hivepro.com