MAG212 CYBER

DAILY

DAILY CYBER INTELLIGENCE

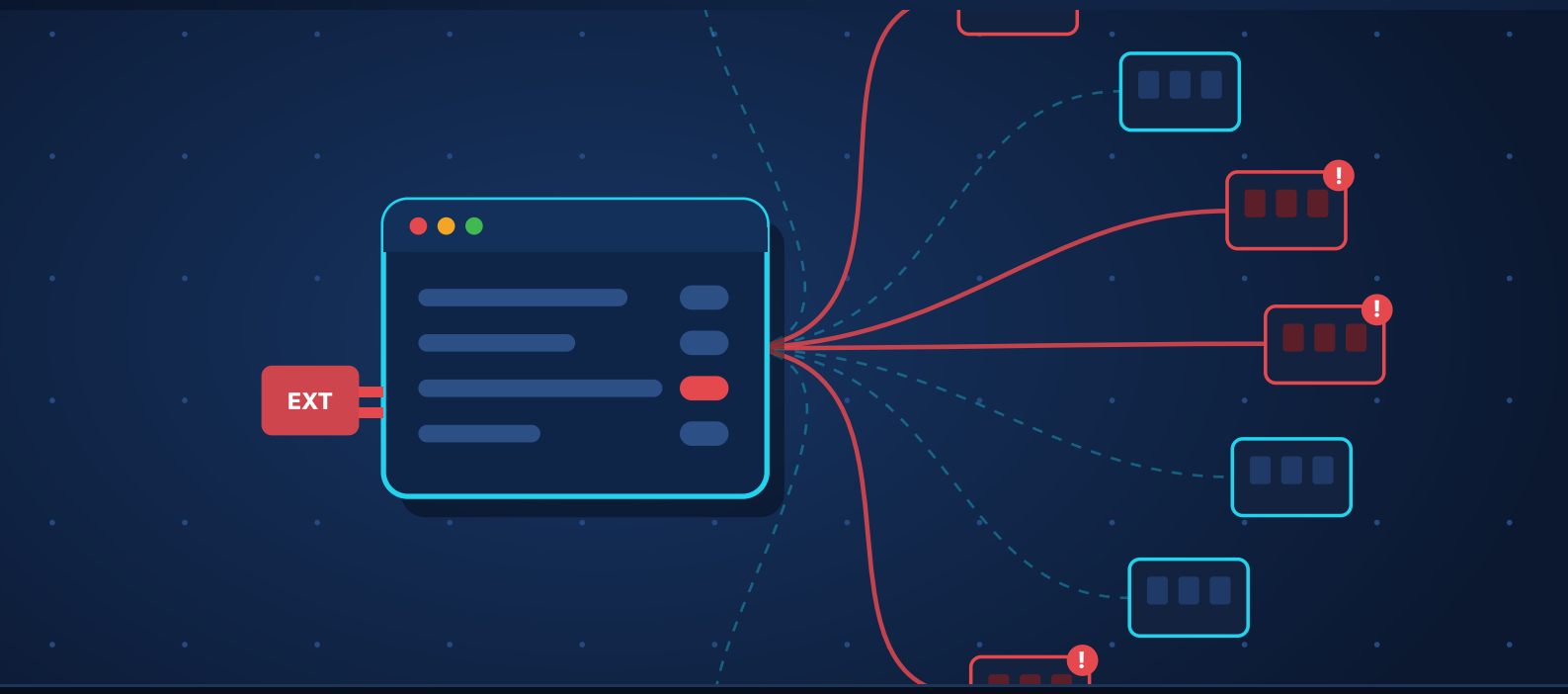
Thursday 12 November 2026

Research cutoff: 06:00 PT (14:00 UTC) · Stories from the 24 h before 06:00 PT, extended to 72 h where labelled

Trusted tools, hostile hands

Attackers turned MSPs' own ScreenConnect consoles against their customers through a suspect extension, four KEV deadlines land today, and an AI pentest platform shows up in real intrusions that reached AWS secrets.

- **ScreenConnect**: SCKit hits 288 endpoints in 90 min · RMM+ extension suspected
- **Zoom Workplace** 9.6 flaw · update Windows to 7.1.8
- **AntiFox** AI pentest tool linked to AWS secret reads
- **KEV due today**: OpenSSH, GPUStack, FreeSWITCH, Aspera Faspex
- **Qlik Sense** servers used to stage ActiveMQ and Veeam exploits
- **Apache httpd** HTTP/2 9.8 · Ivanti EPM 9.8 · eMudhra 16 Nov



By **El Mostafa Ouchen** · cyber.mag212.com

Free subscription: cyber.mag212.com/subscribe-free

Cover art: conceptual illustration, MAG212 CYBER original. Not a real system.

Executive briefing

MAG212 ANALYSIS The past 24 hours were about **trusted tools used against the people who trust them**. Attackers used MSPs' own cloud ScreenConnect consoles to push rogue remote-access clients and a toolkit called SCKit to at least 288 customer machines in 90 minutes, possibly through a weakness in a third-party extension rather than ScreenConnect itself. An open-source AI pentesting platform turned up in intrusions that read a production AWS secret. And Qlik Sense's scheduler again became a launch pad. Meanwhile four CISA KEV deadlines fall **today**, with Barracuda's tomorrow.

The three actions that matter most today

1

MSPs and their customers: hunt rogue ScreenConnect clients, don't remote in

Don't open interactive sessions to suspect devices; investigate with separate tooling. Keep the five disabled extensions off, review Run Command and Toolbox history, revoke sessions and reset credentials from a clean device. Look for client IDs `2588ef5c15954b10` and `ed630cc2c873b091` and a **TrapWatch** scheduled task; keep infected hosts isolated until fully cleaned. ↗ Sophos ↗ The Hacker News

2

Close out today's KEV four

OpenSSH 10.6p2 on musl/Alpine (or `PasswordAuthentication no`), GPUStack 2.2.2, FreeSWITCH 1.11.3, Aspera Faspex 5.0.19 PL1. CISA flags these for forensic triage: check for compromise, not just the version. ↗ CISA KEV

3

Patch the wide-footprint criticals this week

Zoom Workplace for Windows 7.1.8; Apache httpd 2.4.71 (or drop `h2` / `h2c`); Ivanti EPM 2024 SU8 and CSA 5.0.8.1. None is reported exploited yet. ↗ Zoom ↗ The Hacker News ↗ SecurityWeek

Story board

#	Story	Date label	Exploited?	Who should care
1	ScreenConnect / SCKit MSP campaign	11–12 Nov	YES	MSPs and every client of one
2	KEV deadline day: four flaws	KEV 9 Nov, due 12 Nov [72h]	YES	Linux, AI/GPU, VoIP, file-transfer admins
3	Zoom Workplace for Windows	10 Nov [72h]	NO	Every Windows fleet
4	Qlik Sense reverse shells	11 Nov	ATTEMPTED	BI/analytics owners, backup admins
5	AntiFox and AWS secrets	10–11 Nov	YES	Cloud, web and IIS teams
6	Apache httpd HTTP/2 flaw	11–12 Nov	DISPUTED	Web hosting, schools, appliances
7	Ivanti EPM/CSA, Citrix XenServer	10–11 Nov	NO	Endpoint and virtualisation admins
8	Deadlines and follow-ups	13–30 Nov	SOME	Everyone with a calendar

Labels: CONFIRMED primary source · REPORTED secondary outlet · CLAIMED attacker or unverified · MAG212 ANALYSIS our judgement · UNKNOWN not established. [72h] = older than 24 hours, included because it matters today.

In this issue

01 **Attackers turn MSPs' ScreenConnect consoles on their customers** 4
SCKit · RMM+ blank-key weakness suspected · no CVE

02 **Four exploited flaws hit their KEV deadline today** 6
OpenSSH · GPUStack · FreeSWITCH · Aspera Faspex

03 **Zoom Workplace for Windows needs 7.1.8** 8
CVE-2026-108186 (9.6) and -108187 (8.1)

04 **Qlik Sense servers used as a staging post** 9
Reverse shells · ActiveMQ and Veeam exploits staged

05 **An AI pentest platform shows up in real intrusions** 10
AntiFox · IIS web shell · AWS GetSecretValue

06 **Apache httpd 2.4.71 fixes a Critical HTTP/2 flaw** 12
Plus mod_md and mod_vhost_alias fixes · exploit status disputed

07 **Ivanti and Citrix ship critical fixes** 13
EPM SU8 · CSA 5.0.8.1 · XenServer

08 **Deadlines and follow-ups to 30 November** 14
Barracuda · Xen Orchestra · eMudhra · Asus

◆ **Defender's Action Desk** 15
Checklist · KEV deadlines · pending items

◆ **Awareness lesson and briefly noted** 16
"A support app you didn't expect is a reason to call, not click"

◆ **Source register** 17
70 sources, with whether we opened them

↻ Updates to yesterday's stories

- **KEV: nothing new.** CONFIRMED CISA's catalog was still at version 2026.11.10 at research time; no additions on 11 or 12 November. ↗ CISA KEV
- **Xen Orchestra: second advisory, still no CVE.** CONFIRMED Vates published VSA-2026-063 ("crafted keys through XO vm.import privilege", Important) the same day as the exploited VSA-2026-062; neither carries a CVE. Yesterday's actions stand. See story 8. ↗ Vates
- **OpenSSH SSHole: exploitation detail.** REPORTED Previdian saw a first attempt less than nine hours after disclosure and confirmed root on an Alpine honeypot; SecurityWeek reports botnets and cryptominers using it. ↗ Help Net Security ↗ SecurityWeek
- **N-able N-central:** UNKNOWN We could not confirm whether the hotfix has shipped or service is restored. Check the vendor status page before reconnecting on-prem servers.

ACTIVE CAMPAIGN · MSPS AND THEIR CUSTOMERS

01

Attackers turn MSPs' ScreenConnect consoles on their own customers

Active | No CVE · patching won't fix it | Don't remote in | 11–12 Nov

Evidence: strong (Sophos, Huntress, ConnectWise)

SCALE (HUNTRESS)	SUSPECTED WAY IN	PAYLOAD	VENDOR ACTION
288+ endpoints · 48+ organisations · in about 90 minutes	RMM+ extension 1.0.31/1.0.32 accepts a blank key	Rogue clients + SCKit (16 files, TrapWatch task)	5 third-party extensions disabled; ~400 environments had one

What happened

CONFIRMED Sophos X-Ops is investigating unauthorised ScreenConnect client deployments. It saw **three compromised ScreenConnect instances** used to run commands and **two malicious instances** receiving the new clients, and notes that ConnectWise has confirmed the incident and advised disabling the extensions under investigation. ↗ Sophos

REPORTED Huntress first saw the activity at about **17:47 UTC on 11 November**. Attackers used **Run Command** on cloud-hosted ScreenConnect panels to install rogue clients on **at least 288 endpoints in 48 organisations**, all within about 90 minutes and roughly a third in the first ten. Huntress's first count on Reddit was six MSPs. The rogue clients deliver **SCKit**, a 16-file toolkit. ↗ The Hacker News ↗ The Register ConnectWise disabled five extensions (**Labtech Plus, RMM Plus, RMM+, RMM Plus Password Link, RMM+ Password Link**) where it could, and found about 400 partner environments with at least one installed; that is not a count of victims. ↗ BleepingComputer

REPORTED **Likely way in.** Huntress traced the activity to a **possible authentication weakness in RMM+**, an extension that lets other tools send commands through ScreenConnect without using the console. Versions 1.0.31 and 1.0.32 accept a blank access key when none has been set, and work outside ScreenConnect's own logins and MFA. Its investigators saw commands arrive with no matching logins. Attacks hit ScreenConnect 26.6.6.9747 and 26.7.6.9783, so being on the latest release didn't protect anyone. ↗ The Register ConnectWise says it has found no evidence of a compromise of its own infrastructure or of a ScreenConnect vulnerability, and that initial access is still under investigation. **No CVE is assigned.** Its November advisory wasn't on the public advisories index when MAG212 checked. ↗ The Hacker News ↗ ConnectWise

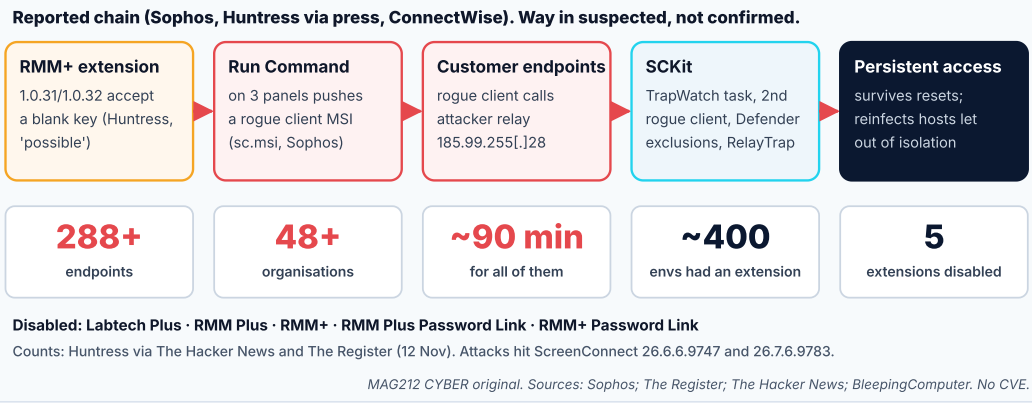


Figure 1 · How the ScreenConnect campaign reached customers. From a suspected RMM+ weakness to persistent access, with Huntress's counts. The way in is suspected, not confirmed, and there is no CVE.
MAG212 CYBER original diagram, based on Sophos, The Register, The Hacker News and BleepingComputer (11–12 Nov 2026).

Who is affected and how it works

REPORTED MSPs whose ScreenConnect has one of the five extensions, especially RMM+, and every organisation they manage. ConnectWise says having an extension doesn't mean a partner was compromised, that disabling it doesn't remove access already gained, and that on-prem owners must disable the extensions themselves. ↗ BleepingComputer CONFIRMED In one case Sophos saw `curl.exe` download the client to `C:\Windows\TEMP\sc.msi`, `msiexec.exe` install it silently, then PowerShell with an execution-policy bypass fetch a second-stage script. ↗ Sophos REPORTED SCKit adds Defender exclusions, installs a second attacker-controlled client, creates a scheduled task named **TrapWatch** and replaces the genuine

ScreenConnect install with an attacker copy. A component Huntress calls RelayTrap waits for a technician to connect, to steal session cookies and pivot to other panels; Huntress rebuilt that step from code and hasn't seen it succeed. Some machines were **reinfected within minutes of leaving isolation.** ↗ The Hacker News ↗ The Register

What to look for

Type	Indicator (defanged)	Note
Relay IP	`185.99.255[.]28`	Hostname "screen"; serves the MSI
C2	`newnewnew.gotdns[.]org` · `soxnewwork.homedns[.]org`	Possible: `cdn007-digitaldownloads[.]com`
Secondary C2	`sc.payproofkit[.]com` (`155.94.150[.]39`)	Hostname WIN-FB5CKHMU4E1
Stager	`hxxps://ns.mo7sen[.]dev/EadF.php?p=4`	PowerShell second stage
Malicious instance IDs	`2588ef5c15954b10` · `ed630cc2c873b091`	Sophos; the second also appears in a July sample
Compromised instance IDs	`d905b2b1b165d0a9` · `4b8f4089ddaac6a9` · `df1f7ef0cfacd0d8`	Sophos: panels used to push the clients
SCKit artefacts	`sckit-run.bat` · `sckit-decoder.ps1` · `TrapWatch.ps1` · `Sqlite3.exe` · task **TrapWatch** · `C:\ProgramData\RelayTrap\` · Run key `RelayTrapLiteAlert`	Huntress via The Hacker News; folder and Run key per IT Security Guru
Installer	`/Bin/ScreenConnect.ClientSetup.msi?…&c=Exploited<N>` · `C:\Windows\TEMP\sc.msi`	Sequential numbering
Account / files	`Addmin` · `Panel-Lateral.ps1` · `runnew.cmd` · `ToolboxRelayUploader.exe` · `Run-Lateral-Full.bat`	Purpose not described

Sources: Sophos; Huntress via BleepingComputer and The Hacker News; IT Security Guru. Huntress's own post was not opened by MAG212. **REPORTED** BleepingComputer also found a July 2026 sample, `SSA-2026-STATEMENT-15518787.bat`, that references the second client ID; any link to this campaign is unclear.

Endpoint sweep OS: Windows 10/11, Server 2016+ Shell: PowerShell 5.1 Privileges: local administrator **READ-ONLY**

```
# ScreenConnect client services: the ID in brackets is the instance the client reports to
Get-CimInstance Win32_Service | Where-Object { $_.Name -like 'ScreenConnect Client (*' } |
  Select-Object Name, State, PathName
# Live connections to the published relay / secondary C2
Get-NetTCPConnection -RemoteAddress 185.99.255.28,155.94.150.39 -ErrorAction SilentlyContinue
# Recently resolved names that match the published domains
Get-DnsClientCache | Where-Object { $_.Entry -match
'gotdns\.org|homedns\.org|payproofkit|mo7sen|cdn007-digitaldownloads' }
# Published file names, and Defender exclusions added by the operator
Get-ChildItem C:\Users,C:\ProgramData,C:\Windows\Temp -Recurse -File -ErrorAction SilentlyContinue `
  -Include Panel-Lateral.ps1,runnew.cmd,ToolboxRelayUploader.exe,Run-Lateral-Full.bat,sckit-
*,TrapWatch.ps1
Get-MpPreference | Select-Object ExclusionPath, ExclusionProcess
# SCKit persistence: TrapWatch task, RelayTrap folder, staged installer, Run key
Get-ScheduledTask -TaskName 'TrapWatch*' -ErrorAction SilentlyContinue
Test-Path 'C:\ProgramData\RelayTrap', 'C:\Windows\Temp\sc.msi'
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v RelayTrapLiteAlert 2>$null
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v RelayTrapLiteAlert 2>$null
```

Expected clean result: only your MSP's own client ID in the service list, `False False` from Test-Path, and no output from the other commands. Any service ID you don't recognise, or either published ID, is a hit: isolate the device using your EDR, not ScreenConnect. **Commands not tested by MAG212 CYBER.** Indicators from Sophos and Huntress via The Hacker News.

Investigate, contain and remediate (in order)

1. **Don't open interactive ScreenConnect sessions** to any device that may be compromised. Investigate with separate security tools. (ConnectWise)

2. **Keep the five extensions disabled**, RMM+ above all; on-prem servers, disable them yourself. Keep their installation records and logs. Don't re-enable until ConnectWise says so.
3. **Review** authentication logs, extension installation records, admin activity, **Run Command history and Toolbox records**, back to before 11 November.
4. **Revoke active sessions, reset credentials from a trusted device, verify MFA** on every ScreenConnect account. ↗ BleepingComputer
5. **Isolate and clean infected hosts completely** before reconnecting: rogue clients, the TrapWatch task, the RelayTrap folder, SCKit files and the RelayTrapLiteAlert Run key. Huntress saw reinfection within minutes of isolation ending. ↗ The Register ↗ IT Security Guru
6. MAG212 ANALYSIS Check that the genuine ScreenConnect client is still the one running; SCKit replaces it with an attacker copy. Reimage confirmed hits if in doubt, and check technician workstations too.
7. MAG212 ANALYSIS Customers: ask your MSP today whether it uses ScreenConnect, whether any of the five extensions were enabled, and what it has checked on your machines.

Verify recovery: every endpoint shows only approved ScreenConnect client IDs; no traffic to the indicators for 72 hours; Run Command history reviewed and signed off; all operator sessions re-established after the credential reset. **Prevention** MAG212 ANALYSIS : treat RMM extensions like code you deploy to every customer. An extension with its own API key can sidestep your MFA: keep an approved list, set strong keys on every integration API, restrict operator logins by IP, and alert on Run Command used outside change windows.

ACTIVELY EXPLOITED · LINUX, AI/GPU, VOIP, FILE TRANSFER

02

Four exploited flaws hit their KEV deadline today

Exploited | Due 12 Nov | Forensic triage | KEV 9 Nov [72h] | Evidence: strong

OPENSSH	GPUSTACK	FREESWITCH	ASPERA FASPEX
CVE-2026-123158 · 8.1 · fix 10.6p2	CVE-2026-102895 · 9.8 · fix 2.2.0 (2.2.2 advised)	CVE-2026-116779 · 9.8 · fix 1.11.3	CVE-2026-123218 · 9.8 · fix 5.0.19 PL1

What happened

CONFIRMED CISA added all four to the Known Exploited Vulnerabilities catalog on **9 November with a 12 November due date**. Ransomware use is "Unknown" for each. Federal agencies must fix them today; for everyone else, a three-day clock means CISA sees real risk. ↗ CISA KEV

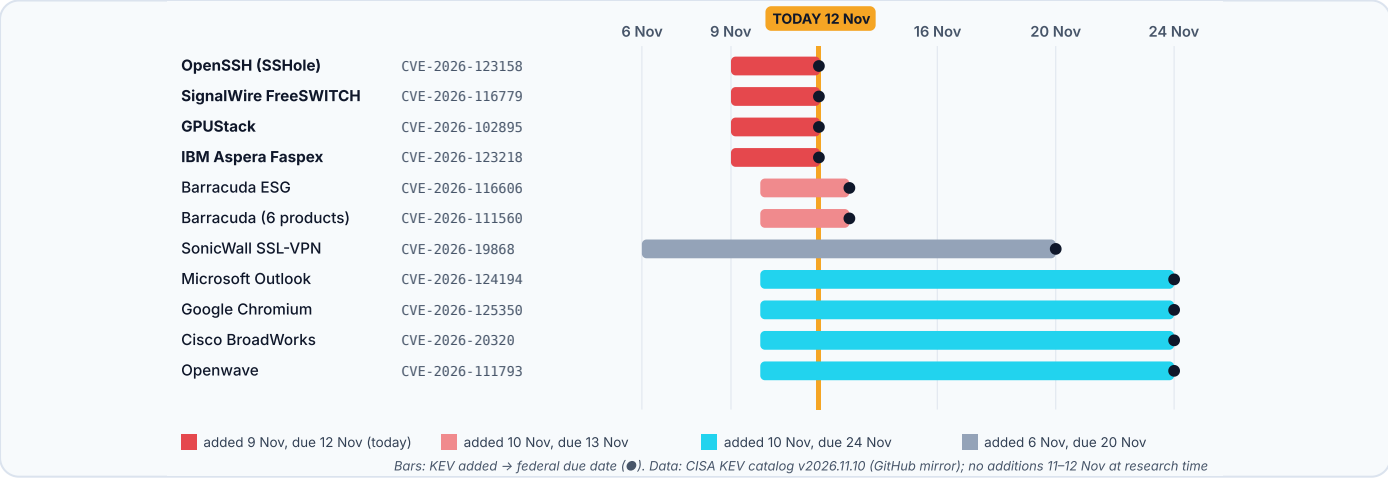


Figure 2 · KEV clocks: four due today. Each bar runs from the date CISA added the flaw to the federal due date. Red bars end today. *MAG212 CYBER original chart. Data: CISA KEV catalog v2026.11.10 (GitHub mirror).*

Who is affected and how each works

Product	Affected	How it works	Fix / workaround
OpenSSH "SSHole"	sshd before 10.6p2 on **musl libc without PAM** (Alpine is the main case)	sshd misreads whether a string is a password hash; with some account setups any 256–1024-character password is accepted. CONFIRMED ↗ Tenable	10.6p2, or `PasswordAuthentication no`. Rebuild container images.
GPUStack	Before 2.2.0 (advisory GHSA-gj9m-f8ph-pmhr, 31 Jul; the advisory itself lists no CVE)	With the default `force_auth_localhost=false`, loopback requests get admin; behind a same-host proxy every request looks local, and a spoofed `X-GPUStack-Real-IP` works. Attackers used it against a v2.1.1 deployment to create custom backends running reverse shells (reported by Javier Sixto). CONFIRMED ↗ GPUStack advisory	2.2.2 (also fixes SAML flaw CVE-2026-102894); or `force_auth_localhost=true`, strip the header, block `/auth/saml/callback`
FreeSWITCH	1.11.2 and earlier	A SIP MESSAGE that selects the "api" chat protocol reaches the FreeSWITCH API and runs commands. REPORTED ↗ SecurityOnline	1.11.3; keep `enable-chat-api-proto` off, `enable-chat=false`, remove passwordless directory users
IBM Aspera Faspex	5.0.0–5.0.19	A crafted message bypasses authorization for full admin rights. IBM's bulletin says nothing about exploitation; the KEV listing is the evidence. CONFIRMED ↗ IBM	5.0.19 PL1 (faspex-core 1ce4b13, Fix Pack 1). No workaround.

REPORTED SSHole was attacked fast: Previdian saw a first attempt under nine hours after disclosure and confirmed root on an Alpine honeypot. A self-hosting blog argues the root cause lies in musl rather than OpenSSH; for defenders the fix is the same. ↗ Help Net Security ↗ botmonster UNKNOWN Who exploited GPUStack, FreeSWITCH and Faspex; no IOCs have been published for any of the four.

Exposure check OS: Linux (Alpine and others) Shell: sh/bash Privileges: root for sshd -T READ-ONLY

```
# OpenSSH: version, libc and the two settings that decide exposure
ssh -V
ldd "$(command -v sshd)" 2>/dev/null | grep -i musl
sshd -T 2>/dev/null | grep -Ei '^(passwordauthentication|usepam) '
# Recent password logins (Alpine logs to /var/log/messages by default)
grep -h 'Accepted password' /var/log/messages /var/log/auth.log 2>/dev/null | tail -n 50
# FreeSWITCH: version
fs_cli -x 'version'
```

Exposed to SSHole if the version is below 10.6p2, `ldd` shows musl, `passwordauthentication yes` and `usepam no`. Any "Accepted password" for an account that shouldn't use passwords is a lead. **Commands not tested by MAG212 CYBER.**

Contain and remediate (in order)

1. **Inventory** musl-based hosts and images running sshd, GPUStack servers, FreeSWITCH boxes and Faspex instances; take any internet-facing ones off the internet if you can't patch today.
2. **Patch** to the fixed versions above, or apply the workarounds as a stop-gap.
3. MAG212 ANALYSIS **Triage** anything exposed since disclosure: new SSH keys, cron jobs, miners, GPUStack API keys you didn't create, unexpected FreeSWITCH dialplan or Lua changes, Faspex admin accounts.
4. MAG212 ANALYSIS GPUStack exposes cloud-provider and worker secrets: rotate them on any instance that was reachable.

Verify recovery: fixed versions confirmed on every instance; `PasswordAuthentication no` where password login isn't needed; no unexplained accounts or keys. **Prevention** MAG212 ANALYSIS : AI and GPU management servers are now on attackers' lists; put them behind the same access controls as any admin console.

PATCH · ZOOM WORKPLACE FOR WINDOWS

03

Zoom Workplace for Windows needs 7.1.8 to close two privilege-escalation flaws

CVSS 9.6 | Not reported exploited | Published 10 Nov [72h] | Evidence: strong

CVE-2026-108186	CVE-2026-108187	NEEDS	FIX
9.6 · improper input validation · 7.1.0 to before 7.1.8	8.1 · origin validation error · before 7.1.5	User interaction (UI:R), no privileges	7.1.8 or later covers both

What happened

CONFIRMED Zoom's bulletin ZSB-26023 rates **CVE-2026-108186** Critical (CVSS 9.6, vector AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H): improper input validation in Zoom Workplace for Windows that "may allow an unauthenticated user to conduct an escalation of privilege via network access". It affects 7.1.0 up to, but not including, 7.1.8, and was found by Zoom Offensive Security. ZSB-26024 covers **CVE-2026-108187** (8.1, origin validation error) in versions before 7.1.5, reported by "shmoul". Both were published on 10 November. ↗ Zoom ZSB-26023 ↗ ZSB-26024



Figure 3 · Which Zoom builds each flaw affects. Builds 7.1.5 to 7.1.7 fix one flaw but not the other. 7.1.8 or later is the target. *MAG212 CYBER original chart. Data: Zoom bulletins ZSB-26023 and ZSB-26024 (10 Nov 2026).*

Who is affected and how it works

CONFIRMED Windows installs of Zoom Workplace in those ranges. REPORTED Neither Zoom nor the press reports exploitation, and 7.1.8 fixes both. ↗ The Hacker News ↗ SecurityWeek UNKNOWN The exact attack scenario. Both vectors need a user action, such as joining a meeting or clicking a link; we won't guess which. Whether macOS, Linux, VDI or Rooms builds share either flaw isn't stated in what we read.

What to look for, then fix

1. **Find the version** across the fleet with your software inventory or MDM; anything from 7.1.0 to 7.1.7 has the 9.6 flaw, and anything before 7.1.5 has both.
2. **Push 7.1.8 or later** and turn on Zoom's auto-update where users install it themselves.
3. MAG212 ANALYSIS No indicators exist. Until patched, watch for Zoom processes spawning shells or writing to system folders.

Verify recovery: the inventory shows no Windows build below 7.1.8. **Prevention** MAG212 ANALYSIS : user-installed per-user Zoom copies often escape central patching; block them or bring them under management.

INTRUSIONS · QLIK SENSE ENTERPRISE FOR WINDOWS

04

Qlik Sense servers used as a staging post for ActiveMQ and Veeam exploits

Attempted · blocked | Entry flaw unknown | Reported 11 Nov | Evidence: medium (Cynet via press)

RESEARCHER	SEEN	INFRASTRUCTURE	NEXT TARGETS STAGED
Cynet CyOps and Research	October 2026 · several EU customers in ~3 minutes	45.115.26[.]23 · ports 4455, 4456, 8012	ActiveMQ CVE-2023-46604 · Veeam CVE-2024-40711

What happened

REPORTED Cynet's CyOps and research teams found Qlik Sense servers at **several EU-based customers** trying to launch PowerShell reverse shells to `45.115.26[.]23` in October, all within a window of just over three minutes. The initial command was Nishang's one-line reverse shell, run under Qlik's `scheduler.exe`; Cynet blocked the spawn attempts. An open directory on the same IP held a Go backdoor, SSH persistence scripts, an Apache ActiveMQ CVE-2023-46604 exploit and a modified Veeam CVE-2024-40711 toolchain. ↗ The Hacker News ↗ Mallory Cynet has published its research; MAG212 found it but couldn't open it, so the details come through the press. ↗ Cynet

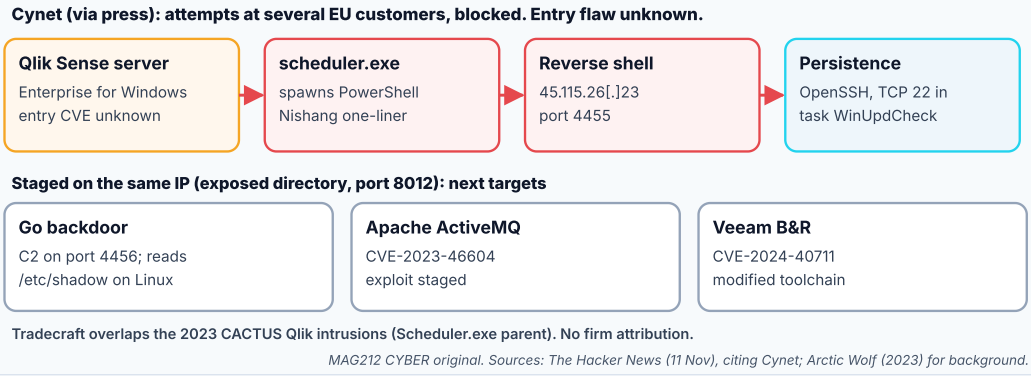


Figure 4 · From Qlik's scheduler to staged exploits. The reported chain, which Cynet blocked, and what sat in the attacker's open directory. The Qlik entry flaw is unknown.
MAG212 CYBER original diagram, based on The Hacker News (11 Nov 2026) citing Cynet.

Who is affected and how it works

REPORTED Internet-facing Qlik Sense Enterprise for Windows servers. **Which Qlik flaw was used isn't known.** The likely candidates are the 2023 trio: CVE-2023-41265 (HTTP tunnelling), CVE-2023-41266 (path traversal) and CVE-2023-48365 "DoubleQlik", an incomplete fix for the first. The persistence script installs a legitimate OpenSSH package, sets `sshd` to start automatically, opens inbound TCP 22, and runs `C:\ProgramData\ssh\winc.ps1` from a task named **WinUpdCheck** every five minutes. On Linux the Go backdoor reads `/etc/shadow` and `/etc/passwd` and looks for running ActiveMQ. ↗ The Hacker News

MAG212 ANALYSIS The scheduler.exe parent matches the 2023 CACTUS ransomware intrusions documented by Arctic Wolf, but nobody has attributed this activity. ↗ Arctic Wolf (2023)

Qlik host check OS: Windows Server Shell: PowerShell 5.1 Privileges: local administrator READ-ONLY

```
# Persistence artefacts named in the report
Get-ScheduledTask -TaskName 'WinUpdCheck' -ErrorAction SilentlyContinue
Test-Path 'C:\ProgramData\ssh\winc.ps1'
Get-Service sshd -ErrorAction SilentlyContinue
# Connections to the reported C2
Get-NetTCPConnection -RemoteAddress 45.115.26.23 -ErrorAction SilentlyContinue
# Process-creation events with Qlik's scheduler as parent (needs 4688 auditing)
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4688} -MaxEvents 20000 -ErrorAction
SilentlyContinue |
  Where-Object { $_.Message -match 'Scheduler\.exe' -and $_.Message -match 'powershell|cmd\.exe' } |
  Select-Object TimeCreated, Message
```

Expected clean result: no task, `False`, no sshd service (unless you installed one), no connections, no events. **Commands not tested by MAG212 CYBER.** Indicators from The Hacker News, citing Cynet.

Contain and remediate (in order)

1. **Take Qlik Sense off the internet** or put it behind VPN or SSO; block `45.115.26[.]23`.
2. **Patch Qlik Sense** to a release that fixes all three 2023 CVEs (see Qlik's support articles). ↗ Qlik
3. **Run the host check**; on a hit, remove the task, script, sshd service and TCP 22 rule, rotate the Qlik service account and rebuild.
4. MAG212 ANALYSIS **Check the next targets**: ActiveMQ patched for CVE-2023-46604, Veeam Backup & Replication for CVE-2024-40711. Neither should be reachable from the Qlik server.

Verify recovery: Qlik build confirmed; no scheduler.exe-spawned shells for 7 days; ActiveMQ and Veeam versions checked.
Prevention MAG212 ANALYSIS : three-year-old Qlik bugs are still paying off for attackers. Analytics servers are often forgotten in patch cycles, so add them to yours.

INTRUSIONS · IIS, AWS

05 An AI pentest platform shows up in real intrusions that read an AWS production secret

Exploited | File-pattern IOCs only | Arctic Wolf 10 Nov [72h] | Evidence: medium–strong

RESEARCHER	TOOL	HOSTING	IMPACT
Arctic Wolf Labs, Adversary Research	AntiFox: open-source, Chinese-language agentic pentesting	Alibaba Cloud hosts serving AntiFox interfaces	≥1 successful GetSecretValue on a production secret

What happened

CONFIRMED Arctic Wolf says it is tracking attackers running self-hosted agentic pentesting frameworks, including AntiFox, from public cloud. In several recent intrusions, **Alibaba Cloud systems hosting AntiFox interfaces** were tied to confirmed malicious actions against internet-facing web services and the AWS environments behind them, chaining web exploitation, web shells, config discovery, credential checks, cloud enumeration, secret access and storage operations. ↗ Arctic Wolf

REPORTED The attackers used valid IAM users and, in some cases, an assumed EC2 role. In one intrusion they cycled through several identities and made hundreds of API calls in about 30 minutes. AntiFox began as a fork of ARTEX 0.1.1, the framework Datadog reported in AWS attacks in October. ↗ BleepingComputer ↗ GBHackers ↗ Datadog MAG212 ANALYSIS "Linked to" means the tool was used; no threat actor is named and the maintainers aren't accused. Public-cloud addresses can be reassigned, as Arctic Wolf warns.

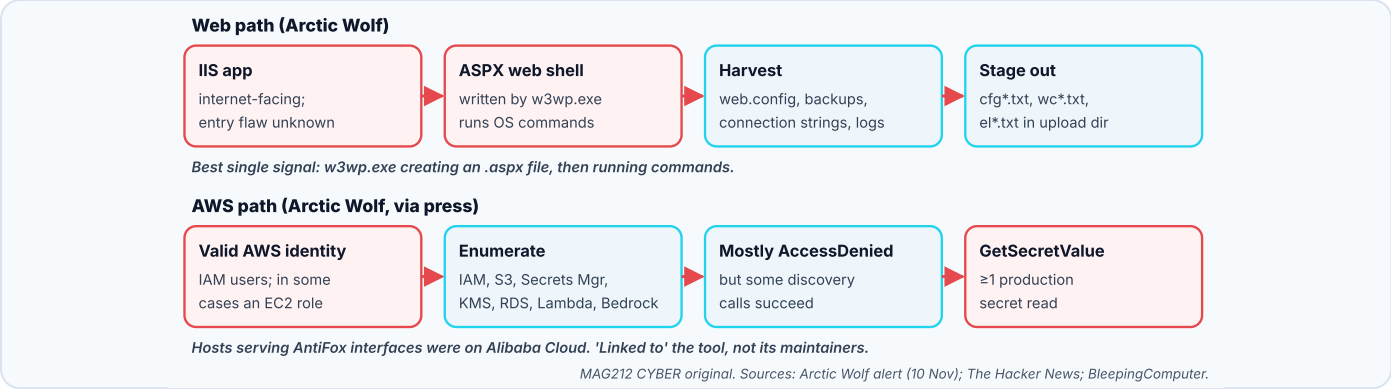


Figure 5 · AntiFox-linked intrusions: two paths. The web path through an IIS web shell and the AWS path from a valid credential to a production secret.
MAG212 CYBER original diagram, based on Arctic Wolf's alert (10 Nov 2026), The Hacker News and BleepingComputer.

Who is affected and how it works

REPORTED **Web:** on a compromised IIS application (entry flaw unknown), `w3wp.exe` wrote an ASPX web shell and ran commands through it, hunted for `web.config` files and backups, read connection strings and logs, tried an internal production database, and copied files into a web-accessible upload folder. **AWS:** starting from a valid credential (origin not stated), the actor enumerated IAM, S3, Secrets Manager, KMS, RDS, Lambda and Bedrock. Most calls returned AccessDenied, but some succeeded, including at least one `GetSecretValue` on a production secret. ↗ The Hacker News CONFIRMED Arctic Wolf's alert lists file patterns in the web-accessible upload folder: `*.aspx`, `pwn*.aspx`, `cfg*.txt`, `wc*.txt`, `el*.txt`, and the AntiFox console title "AntiFox — 自主渗透测试控制台". ↗ Arctic Wolf

Cloud and IIS hunt OS: any (AWS CLI v2) · Windows for IIS Shell: bash · PowerShell Privileges: cloudtrail:LookupEvents · local admin
READ-ONLY

```
# Who read secrets since 1 Oct (management events, per region, last 90 days)
aws cloudtrail lookup-events --region us-east-1 \
  --lookup-attributes AttributeKey=EventName,AttributeValue=GetSecretValue \
  --start-time 2026-10-01T00:00:00Z \
  --query 'Events[].[EventTime,Username,CloudTrailEvent]' --output text | head -n 200
# PowerShell on the IIS server: .aspx files written in the last 30 days
Get-ChildItem C:\inetpub -Recurse -Include *.aspx,*.ashx,cfg*.txt,wc*.txt,el*.txt -File -ErrorAction
SilentlyContinue |
  Where-Object LastWriteTime -gt (Get-Date).AddDays(-30) | Select-Object FullName, LastWriteTime
```

Look for principals or source IPs you don't recognise, especially Alibaba Cloud ranges. Repeat per region. Any new .aspx you didn't deploy, or `pwn*.aspx`, `cfg*.txt`, `wc*.txt` or `el*.txt` in an upload folder, is a lead (Arctic Wolf patterns). **Commands not tested by MAG212 CYBER.**

Contain and remediate (in order)

1. MAG212 ANALYSIS **Alert on** w3wp.exe creating .aspx files or spawning cmd/PowerShell, and on one identity making a burst of List/Describe calls across many services with a high AccessDenied rate.
2. **Revoke affected sessions and access keys, and rotate** any secret read by an unexpected principal and every credential in a harvested `web.config`; this is Arctic Wolf's advice. In CloudTrail, look for the few successful calls inside bursts of denials. ↗ GBHackers ↗ BleepingComputer
3. **Remove long-lived access keys** and cut IAM permissions to what each workload uses; restrict `secretsmanager:GetSecretValue` by resource.

Verify recovery: rotated secrets in use and old values revoked; no unknown principals in CloudTrail for 7 days; web roots match deployed builds. **Prevention** MAG212 ANALYSIS : AI agents make noisy, broad enumeration cheap. That noise is your detection opportunity, if CloudTrail goes somewhere someone watches.

PATCH · APACHE HTTP SERVER

06

Apache httpd 2.4.71 fixes a Critical HTTP/2 flaw; exploit status is disputed

Apache: Critical · Red Hat 9.8 | Exploitation disputed | Released 11 Nov | Evidence: strong

CVE	AFFECTED	FIX	WORKAROUND
CVE-2026-119618 · mod_http2 · Apache: Critical	httpd 2.4.55–2.4.70 with h2/h2c; mod_h2 2.0.8–2.0.42	httpd 2.4.71	Remove h2/h2c from Protocols (Wiz)

What happened

CONFIRMED Apache rates CVE-2026-119618 **Critical**: improper synchronisation of a shared resource in mod_http2's `assign_headers()` can cause heap corruption and remote code execution. It affects httpd 2.4.55 to 2.4.70 and the standalone mod_h2 2.0.8 to 2.0.42, and is fixed in **2.4.71, released 11 November**. Anthropic's OSS Scanner reported it on 26 October and Google Cloud Vulnerability Research (Anthony Weems, Simon Scannell) on 3 November. The same release fixes **CVE-2026-106023** (Important: mod_md NULL dereference crashes a child process, 2.4.30–2.4.70) and **CVE-2026-109163** (Low: mod_vhost_alias one-byte stack overwrite). ↗ Apache

REPORTED Red Hat scores it 9.8 but rates it "Important" on RHEL 9 and 10 because of per-stream memory allocators.

UNKNOWN Whether it is exploited: Red Hat says public research has shown a reliable exploit, without citing it; Wiz says no exploit is available and none has been seen in the wild. ↗ The Hacker News

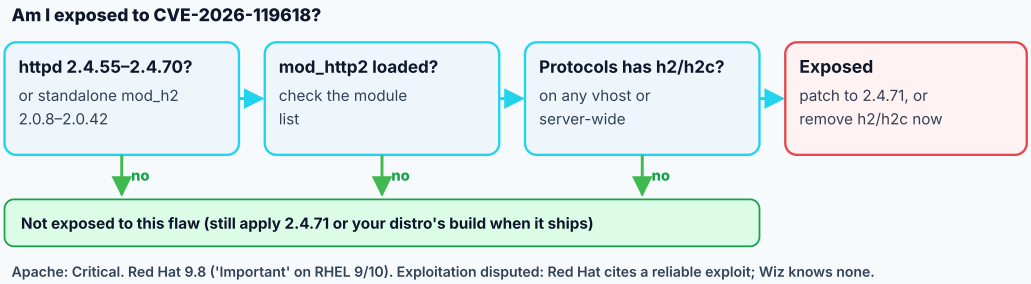


Figure 6 · Am I exposed to CVE-2026-119618?. Three questions decide exposure. Any 'no' means this flaw doesn't apply. *MAG212 CYBER original diagram, based on Apache's security page and The Hacker News (11–12 Nov 2026).*

Who is affected

REPORTED Only servers in the version range **with HTTP/2 enabled** through the `Protocols` directive.

MAG212 ANALYSIS That still covers many school, SMB and hosting servers, and appliances that bundle httpd, whose vendor patches will lag upstream.

Exposure check OS: Linux (Debian/Ubuntu or RHEL family) Shell: bash Privileges: user (root to read some configs)

READ-ONLY

```
# Version (apache2ctl on Debian/Ubuntu, apachectl on RHEL)
apachectl -v 2>/dev/null || apache2ctl -v
# Is mod_http2 loaded?
(apachectl -M 2>/dev/null || apache2ctl -M) | grep -i http2
# Where is HTTP/2 switched on?
grep -RniE '^\s*Protocols\s' /etc/apache2 /etc/httpd 2>/dev/null
```

Exposed only if all three match: a version in range, http2_module listed, and a Protocols line containing h2 or h2c. Distribution packages may carry a backported fix under an older number: check your vendor's advisory. **Commands not tested by MAG212 CYBER.**

Remediate

1. **Update to 2.4.71** or your distribution's fixed package.
2. **Until then**, remove `h2` and `h2c` from Protocols and reload; clients fall back to HTTP/1.1. There is no official workaround; this is Wiz's suggestion. ↗ The Hacker News
3. **Ask appliance vendors** whether their bundled httpd is affected.

Verify recovery: `apachectl -v` shows the fixed build, or an HTTP/2 test (for example `curl -sI --http2 https://your.site`) shows HTTP/1.1. **Prevention** MAG212 ANALYSIS : keep a list of every server that bundles a web server, including appliances, so the next httpd bug takes minutes to scope.

PATCH · IVANTI EPM, CSA, SENTRY · CITRIX XENSERVER

07

Ivanti and Citrix ship critical fixes for management platforms

Two criticals (9.8, 9.4) | Not reported exploited | 10–11 Nov | Evidence: medium

TOTAL	TOP FIX	CSA	XENSERVER
19 flaws: 13 Ivanti, 6 Citrix	EPM 2024 SU8 (CVE-2026-121653)	5.0.8.1 (CVE-2026-121683)	CTX697316 (CVE-2026-102705)

What happened, who is affected and how it works

REPORTED Ivanti fixed an **Endpoint Manager SQL injection that can lead to unauthenticated remote code execution** (CVE-2026-121653, 9.8; EPM 2024 SU8) and a **Cloud Services Application missing-authentication flaw** that lets an attacker add or delete trusted EPM Core certificate entries (CVE-2026-121683, 9.4; CSA 5.0.8.1). CSA with a dual-NIC setup isn't externally exploitable. A high-severity Sentry RCE (CVE-2026-105425) is also fixed. CONFIRMED Ivanti's own update post says it has no evidence of these flaws being exploited and names four Sentry CVEs (CVE-2026-105425, -105669, -123179, -123181), a User Workspace Manager flaw (CVE-2026-105813) and CVE-2026-121683 for CSA, plus EPM and EPMM advisories. ↗ Ivanti REPORTED Citrix's XenServer update fixes CVE-2026-102705, which could let an attacker infer the pool secret and compromise the host, plus five privilege-escalation and task-termination issues and mitigations for AMD guest-to-host flaws; Citrix doesn't state exploitation. ↗ SecurityWeek MAG212 opened Ivanti's summary post but not the per-product advisories or Citrix's bulletin, so the EPM score and fixed builds come from SecurityWeek. ↗ Citrix

Ivanti and Citrix, 10–11 Nov: what to patch first

Product	CVE	CVSS	Impact	Fixed in	Exploited
Ivanti EPM	CVE-2026-121653	9.8	SQLi → unauth RCE	EPM 2024 SU8	No
Ivanti CSA	CVE-2026-121683	9.4	edit trusted EPM certs	CSA 5.0.8.1	No
Ivanti Sentry	CVE-2026-105425	High	RCE	per Ivanti	No
Citrix XenServer	CVE-2026-102705	High	infer pool secret	CTX697316	Unknown

CSA with a dual-NIC setup is not externally exploitable (Ivanti). 19 flaws in all: 13 Ivanti, 6 Citrix.

MAG212 CYBER original. Sources: Ivanti update post (no exploitation); SecurityWeek (scores, builds, Citrix).

Figure 7 · Ivanti and Citrix: what to patch first. The four flaws that matter most from 19 fixed this week. None is reported exploited. *MAG212 CYBER original chart. Data: Ivanti update post; SecurityWeek (11 Nov 2026).*

What to look for, then fix (in order)

1. **EPM core servers first:** upgrade to 2024 SU8. MAG212 ANALYSIS Ivanti flaws have a history of fast weaponisation once patches are diffed; don't wait for a KEV entry.
2. **CSA:** 5.0.8.1; check whether yours runs single-NIC.
3. MAG212 ANALYSIS **After patching**, review EPM's trusted certificate list for entries you didn't add.
4. **XenServer:** apply CTX697316; keep the management network isolated (the same lesson as this week's Xen Orchestra attacks).

Verify recovery: versions confirmed; EPM certificate list reviewed. **Prevention** MAG212 ANALYSIS : endpoint-management servers can push code to every machine, like the ScreenConnect consoles in story 1. Give them the same isolation as a domain controller.

CONTINUING STORIES · BARRACUDA, XEN ORCHESTRA, EMUDHRA, ASUS

08

Deadlines and follow-ups to 30 November

Barracuda due 13 Nov | eMudhra 16 and 30 Nov | Evidence: mixed

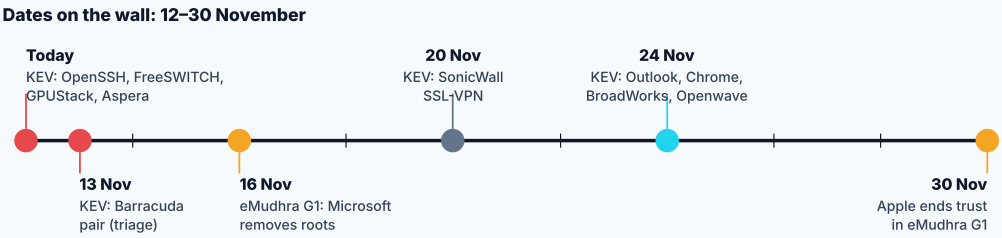


Figure 8 · Dates on the wall, 12–30 November. KEV due dates and the eMudhra distrust milestones on one line. *MAG212 CYBER original chart. Data: CISA KEV v2026.11.10; The Hacker News (11 Nov 2026).*

Barracuda: one day left

CONFIRMED CVE-2026-116606 and CVE-2026-111560 are due **13 November**, with forensic triage flagged. Barracuda's workaround is to restrict the admin UI to trusted networks; patch IDs are on the advisory. No IOCs have been published. ↗ CISA KEV ↗ Barracuda **To do:** confirm patch IDs on every ESG, ADC, BMA, WCC, WAF and WSG; review config-import and restore history on any box whose admin UI was reachable.

Xen Orchestra: exploited, still no CVE

CONFIRMED Vates' VSA-2026-062 (exploited "empty-object" token bypass, root on XCP-ng hosts) still lists no CVE; fixed in XO 6.9.2 and 6.10.1. VSA-2026-063 (Important) was published the same day. Exploitation leaves no log entries, so run the vendor's host checks and block its published IPs and onion C2. ↗ Vates UNKNOWN MAG212 couldn't locate SecurityWeek's 11 November article on these flaws, so we can't say whether it reports VSA-2026-063 as exploited.

eMudhra: certificates stop being trusted

REPORTED After a key-transfer script truncated private keys at an April 2025 key ceremony, eMudhra revoked eight more intermediates (six TLS, two code-signing), using a revocation reason Mozilla participants have questioned. From **16 November** G1 issuance stops, Microsoft starts removing ten eMudhra roots, and Chrome and Firefox distrust G1 certificates issued after that date. Apple ends trust in all G1 certificates on **30 November**. eMudhra reports no known misuse and is leaving public TLS. The main remaining G1 user is "a North American university federation". ↗ The Hacker News ↗ Microsoft MAG212 ANALYSIS **To do:** search your certificate inventory and code-signing chains for emSign/eMudhra issuers and replace them before 16 November. Universities in federated identity schemes should ask their federation today.

Asus routers: four CVEs, none known exploited

REPORTED SecurityWeek says Asus disclosed four high- and medium-severity router firmware flaws that could allow root command execution or memory overwrite. ↗ SecurityWeek CVE records published on 10 November match that count, all for firmware series 3.0.0.4.386, 3.0.0.4.388 and 3.0.0.6.102:

CVE	Flaw	Who can attack	CVSS 4
CVE-2026-88710	OS command injection, root commands	Unauthenticated, adjacent network	8.7
CVE-2026-88707	Out-of-bounds write	Not stated	High
CVE-2026-88709	Command injection via USB device with crafted folder name, root	Physical access	7.0

CVE	Flaw	Who can attack	CVSS 4
CVE-2026-88708	Off-by-one memory overwrite, service crash	Unauthenticated, nearby	5.3

Sources: CVE record mirrors OffSeq, OffSeq, Vulners. Asus's advisory page was not opened by MAG212; fixed firmware builds are listed there.

To do: update router firmware from Asus's advisory page; until then, keep untrusted devices off the router's local network and disable unused USB and remote-admin features. **MAG212 ANALYSIS** Small offices and home workers are the exposure here.

Defender's Action Desk

Prioritised from today's stories. **MAG212 ANALYSIS** for the ordering; sources are in each article.

- [ ] **NOW** **ScreenConnect (MSPs):** no sessions to suspect devices; keep the 5 extensions off (RMM+ first); review Run Command/Toolbox; revoke sessions, reset creds from a clean device, verify MFA. → 01
- [ ] **NOW** **ScreenConnect (customers):** run the endpoint sweep (rogue IDs, TrapWatch, RelayTrap); clean fully before un-isolating; ask your MSP the three questions. → 01
- [ ] **NOW** **KEV due today:** OpenSSH 10.6p2 on musl, GPUStack 2.2.2, FreeSWITCH 1.11.3, Faspex 5.0.19 PL1; triage anything exposed. → 02
- [ ] **TODAY** **Barracuda (due 13 Nov):** patch IDs and config-history review. → 08
- [ ] **TODAY** **Qlik Sense:** off the internet; host check; ActiveMQ and Veeam versions. → 04
- [ ] **TODAY** **AWS:** review GetSecretValue callers since 1 Oct; alert on w3wp.exe writing .aspx. → 05
- [ ] **THIS WEEK** **Patches:** Zoom 7.1.8; httpd 2.4.71 or drop h2/h2c; Ivanti EPM SU8 and CSA 5.0.8.1; XenServer CTX697316. → 03 → 06 → 07
- [ ] **BY 16 NOV** **eMudhra:** replace emSign/eMudhra certificates and code-signing chains. → 08

KEV deadlines (federal due dates; a priority signal for everyone)

CVE	Product	Added	Due
CVE-2026-123158 · -116779 · -102895 · -123218	**OpenSSH · FreeSWITCH · GPUStack · IBM Aspera Faspex**	9 Nov	**12 Nov (today)**
CVE-2026-116606 · -111560	Barracuda	10 Nov	**13 Nov**
CVE-2026-19868	SonicWall SonicOS SSLVPN	6 Nov	20 Nov
CVE-2026-124194 · -125350 · -20320 · -111793	Outlook · Chromium · Cisco BroadWorks · Openwave	10 Nov	24 Nov

Catalog 2026.11.10; no additions on 11–12 Nov at research time. Ransomware use "Unknown" for every entry listed. Source: CISA KEV.

⏳ Pending at the cutoff: check before you act

- **ScreenConnect:** ConnectWise's advisory not on its public index; Huntress's own post not opened. The RMM+ weakness is "possible", with no CVE or fixed version yet.
- **Not opened:** Cynet's Qlik report, Asus advisory (fixed builds), Ivanti per-product advisories, Citrix CTX697316. **N-able:** status unconfirmed.

Awareness lesson: "A support app you didn't expect is a reason to call, not click"

For employees, teachers and students

This week attackers installed remote-support software on hundreds of computers through the IT providers that look after them. ↗ BleepingComputer

- A new remote-support icon, service or pop-up nobody told you about: **call IT on a number you already have**.
- If the mouse moves or windows open on their own, unplug from the network and call.
- Never "allow" access you didn't ask for, even if it names your IT provider.

For leaders and owners

"Your MSP's console is a key to every one of your machines." **MAG212 ANALYSIS**

Ask your MSP in writing which remote tools and extensions it uses on your systems, how operator logins are protected, and how it would tell you about a compromise.

Put the answers in your contract review this quarter.

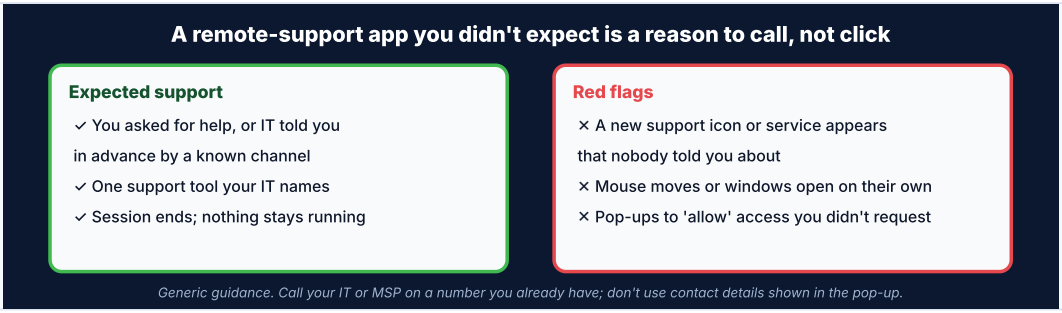


Figure 9 · Expected support versus red flags. What normal remote support looks like, and the signs that it isn't. Generic guidance. *Conceptual MAG212 CYBER original illustration.*

Briefly noted

- **ScreenConnect's earlier CVE.** CONFIRMED Separate from this campaign: CVE-2026-84869, a client flaw that allowed file transfer and execution without host approval, was fixed in 26.6.5 in September and added to KEV. ConnectWise hasn't linked it to the current attacks; on-prem servers should still be on 26.6.5 or later. ↗ Rescana
- **Railway AI keys.** REPORTED Railway says stolen customer AI keys led to about $740,000 in estimated unauthorised usage charges (headline only). ↗ The Hacker News
- **Grok-built apps.** REPORTED More than 35,000 Grok-built apps were found exposed online, some leaking confidential data and passwords (headline only). ↗ The Hacker News
- **Apple.** REPORTED Bluetooth and AirPlay pairing flaws patched across Apple platforms (headline only). ↗ SecurityWeek

Source register

Every source in the research brief; titles link to the source. "No" means not opened, and claims from it rest on the secondary sources listed. "Headline only" items are reported, not verified. Links checked for form; not re-fetched at publication. Corrections: cyber.mag212.com.

1 CISA KEV catalog JSON (official GitHub mirror), catalog 2026.11.10
10 Nov 2026 · Primary (government) · Opened: Yes (coordinator)

2 BleepingComputer: Active ScreenConnect attacks breach MSPs, impact dozens of organizations
11 Nov 2026 · Secondary (quotes Huntress and ConnectWise) · Opened: Yes (coordinator, full read)

3 NetManageIT: syndicated copy of the BleepingComputer ScreenConnect article
11 Nov 2026 · Secondary (syndication) · Opened: Yes

4 ConnectWise Trust Center: advisories index
Latest entry 17 Mar 2026 at fetch · Primary (vendor) · Opened: Yes (no Nov 2026 entry shown)

5 Mallory.ai: ScreenConnect campaign summary including Sophos findings
11-12 Nov 2026 · Secondary (aggregator) · Opened: Yes

6 Sophos: Malicious ScreenConnect deployments observed
11 Nov 2026 · Primary (vendor research) · Opened: Yes (rebuild)

7 QUE.com: Hackers hijacked six MSPs' ScreenConnect consoles
11-12 Nov 2026 · Secondary · Opened: Yes

8 WindowsForum: ScreenConnect attack targets MSPs with rogue clients
11-12 Nov 2026 · Secondary (includes AI-assisted note) · Opened: Yes

9 The Hacker News: ScreenConnect attacks target at least 288 endpoints across 48 organizations
12 Nov 2026 · Secondary · Opened: Yes (rebuild)

10 OT Ecosystem: ScreenConnect cyberattacks, 288 endpoints
Nov 2026 · Secondary · Opened: Search result only

11 Rescana: ConnectWise ScreenConnect CVE-2026-84869 KEV
Sep 2026 · Secondary (background) · Opened: Yes

12 Huntress: Rogue ScreenConnect installations (September campaign)
8 Sep 2026 · Primary (researcher, background) · Opened: Yes

13 SecurityOnline: GPUStack authentication bypass CVE-2026-102895 exploited
5 Nov 2026 · Secondary · Opened: Yes

14 GPUStack GitHub advisory GHSA-gj9m-f8ph-pmhr
Nov 2026 · Primary (vendor) · Opened: Yes (rebuild)

15 SecurityOnline: FreeSWITCH vulnerability CVE-2026-116779 exploited
29 Oct 2026 · Secondary · Opened: Yes

16 Tenable: CVE-2026-123158
Updated 10 Nov 2026 · Secondary (vulnerability database) · Opened: Yes

17 OpenSSH release notes (10.6p2)
5 Nov 2026 · Primary (vendor) · Opened: Yes (10 Nov edition)

18 Alpine Linux: OpenSSH password authentication bypass
5 Nov 2026 · Primary (vendor) · Opened: Yes (10 Nov edition)

19 Help Net Security: OpenSSH sshole exploitation
6 Nov 2026 · Secondary · Opened: Yes (10 Nov edition)

20 SecurityWeek: Hackers exploiting SSHole authentication bypass in OpenSSH
9 Nov 2026 · Secondary · Opened: Listing only

21 botmonster.com: OpenSSH took the blame for musl's Alpine login bug
Nov 2026 · Blog (context) · Opened: Search result only

22 IBM Security Bulletin 7295921: Aspera Faspex authorization bypass
7 Nov 2026 · Primary (vendor) · Opened: Yes

23 Barracuda Trust Center: pre-auth authorization bypass and command injection
2 Nov, updated 9 Nov 2026 · Primary (vendor) · Opened: Yes (11 Nov edition)

24 BleepingComputer: Barracuda warns of critical flaws allowing root access
3 Nov, updated 6 Nov 2026 · Secondary · Opened: Yes

25 SecurityWeek: Recently patched Barracuda vulnerabilities exploited in attacks
11 Nov 2026 · Secondary · Opened: Yes (11 Nov edition)

26 Canadian Centre for Cyber Security: Barracuda advisory AV26-1112
Nov 2026 · Primary (government) · Opened: No

27 Vates VSA-2026-062: Empty-object login token
10 Nov 2026 · Primary (vendor) · Opened: Yes

28 Vates 2026 security advisory index
10 Nov 2026 · Primary (vendor) · Opened: Yes

29 SecurityWeek: Critical Xen Orchestra flaws exploited in attacks
11 Nov 2026 · Secondary · Opened: No (not located)

30 The Hacker News: Hackers target Qlik Sense servers with reverse shells, stage ActiveMQ and Veeam exploits (citing Cynet)
11 Nov 2026 · Secondary · Opened: Yes

31 Qlik: Critical security fixes for Qlik Sense Enterprise for Windows
Aug-Sep 2023 · Primary (vendor, background) · Opened: No

32 VirusTotal: IP 45.115.26.23
n/a · Threat intel · Opened: No (linked by THN)

33 Arctic Wolf: Qlik Sense exploited in Cactus ransomware campaign
Nov 2023 · Primary (researcher, background) · Opened: Search result (coordinator)

34 The Hacker News: AntiFox AI pentesting platform linked to attacks that accessed AWS production secrets (citing Arctic Wolf)
11 Nov 2026 · Secondary · Opened: Yes

35 Arctic Wolf wolf-tools: AntiFox alert pack
Nov 2026 · Primary (researcher) · Opened: Partial (search extract of the GitHub page)

36 Datadog Security Labs: ARTEX agentic attacks in AWS environments
9 Nov 2026 · Primary (researcher, context) · Opened: Yes (coordinator search)

37 Zoom security bulletin ZSB-26023 (CVE-2026-108186)
10 Nov 2026 · Primary (vendor) · Opened: Yes (coordinator)

38 Zoom security bulletin ZSB-26024 (CVE-2026-108187)
10 Nov 2026 · Primary (vendor) · Opened: Yes (coordinator)

39 The Hacker News: Critical Zoom Workplace flaw could allow unauthenticated remote privilege escalation
11 Nov 2026 · Secondary · Opened: Yes

40 SecurityWeek: Asus, Zoom release security patches
11 Nov 2026 · Secondary · Opened: Yes

41 Daily Security Review: Asus CVEs
5 Nov 2026 · Secondary · Opened: Yes

42 Asus security advisory page
Nov 2026 · Primary (vendor) · Opened: No (blocked)

43 The Hacker News: Critical Apache HTTP/2 flaw (CVE-2026-119618)
12 Nov 2026 · Secondary · Opened: Yes

44 Apache HTTP Server 2.4 vulnerabilities page
12 Nov 2026 · Primary (vendor) · Opened: Yes (rebuild)

45 SecurityWeek: Citrix, Ivanti patch critical and high-severity vulnerabilities
11 Nov 2026 · Secondary · Opened: Yes

46 Ivanti: November 2026 security update
10 Nov 2026 · Primary (vendor) · Opened: Yes (rebuild)

47 Citrix CTX697316: XenServer security update for multiple issues
10 Nov 2026 · Primary (vendor) · Opened: No

48 The Hacker News: eMudhra revokes 8 more CAs
11 Nov 2026 · Secondary · Opened: Yes

49 Mozilla Bugzilla 2083449 comment 82
Nov 2026 · Primary (root program) · Opened: No (linked by THN)

50 Microsoft MSRC: Response to compromised eMudhra certificate authority keys
Oct 2026 · Primary (vendor) · Opened: No (linked by THN)

51 Apple support 149555: eMudhra trust changes
Nov 2026 · Primary (vendor) · Opened: No (linked by THN)

52 eMudhra: Certificate security incident notice
Oct-Nov 2026 · Primary (vendor) · Opened: No (linked by THN)

53 RuntimeWire: N-able takes N-central offline after 33 alleged zero-days
9 Nov 2026 · Secondary · Opened: Partial (paywalled lede)

54 GovInfoSecurity: N-able takes platform offline after 33 zero-days drop
10 Nov 2026 · Secondary · Opened: Yes (11 Nov edition)

55 The Hacker News: Railway says stolen customer AI keys led to unauthorized charges
11 Nov 2026 · Secondary · Opened: Listing only

56 The Hacker News: Over 35,000 Grok-built apps exposed online
11 Nov 2026 · Secondary · Opened: Listing only

57 SecurityWeek: Bluetooth, AirPlay pairing vulnerabilities patched across Apple platforms
11 Nov 2026 · Secondary · Opened: Listing only

58 The Register: Hackers exploiting ScreenConnect plugin flaw to spread malware across hundreds of PCs
12 Nov 2026 · Trade press (citing Huntress, ConnectWise) · Opened: Yes (rebuild)

59 Huntress: SCKit worm and rogue ScreenConnect clients
11-12 Nov 2026 · Primary (researcher) · Opened: No (linked by The Hacker News; approval not answered)

60 IT Security Guru: Huntress uncovers SCKit, 288 hosts in 90 minutes
12 Nov 2026 · Trade press · Opened: Search extract only

61 Cynet: Exploiting Qlik Sense servers (research)
11 Nov 2026 · Primary (researcher) · Opened: No (approval not answered)

62 The IT Nerd: Cynet uncovers Qlik Sense attack campaign
11 Nov 2026 · Blog (Cynet statement) · Opened: Search extract only

63 Mallory.ai: Qlik Sense reverse-shell attempts expose attacker tooling
11 Nov 2026 · Aggregator · Opened: Search extract only

64 BleepingComputer: Hackers use AntiFox AI agents in AWS credential-theft attacks
11 Nov 2026 · Trade press (citing Arctic Wolf) · Opened: Search extract only

65 GBHackers: AntiFox AI agents linked to AWS attacks
11 Nov 2026 · Trade press (citing Arctic Wolf) · Opened: Search extract only

66 Security Affairs: AI pentest tool AntiFox abused to steal AWS credentials
11 Nov 2026 · Trade press (citing Arctic Wolf) · Opened: Search extract only

67 Vulners (CVE record mirror): CVE-2026-88708 ASUS router off-by-one
10 Nov 2026 · CVE record mirror · Opened: Search extract only

68 Vulners (CVE record mirror): CVE-2026-88709 ASUS router OS command injection via USB
10 Nov 2026 · CVE record mirror · Opened: Search extract only

69 OffSeq Radar (CVE record mirror): CVE-2026-88710 ASUS router OS command injection
10 Nov 2026 · CVE record mirror · Opened: Search extract only

70 OffSeq Radar (CVE record mirror): CVE-2026-88708, lists related CVE-2026-88707
10 Nov 2026 · CVE record mirror · Opened: Search extract only

MAG212 CYBER

DAILY CYBER INTELLIGENCE

Get tomorrow's briefing before your first coffee

Verified stories, the three actions that matter, and clear labels for what's confirmed, reported and still unknown. Free.

Subscribe free →

cyber.mag212.com/subscribe-free

Verified, not viral
Primary sources first, conflicts flagged, nothing invented.

Built for defenders
Versions, fixes, log locations and ordered remediation steps.

For every team
Network engineers, MSPs, school IT, IT managers and owners.

Editor: **El Mostafa Ouchen** · cyber.mag212.com · Issue MAG212_CYBER_Daily_2026-11-12