MAG212 CYBER

DAILY

DAILY CYBER INTELLIGENCE

Wednesday 11 November 2026

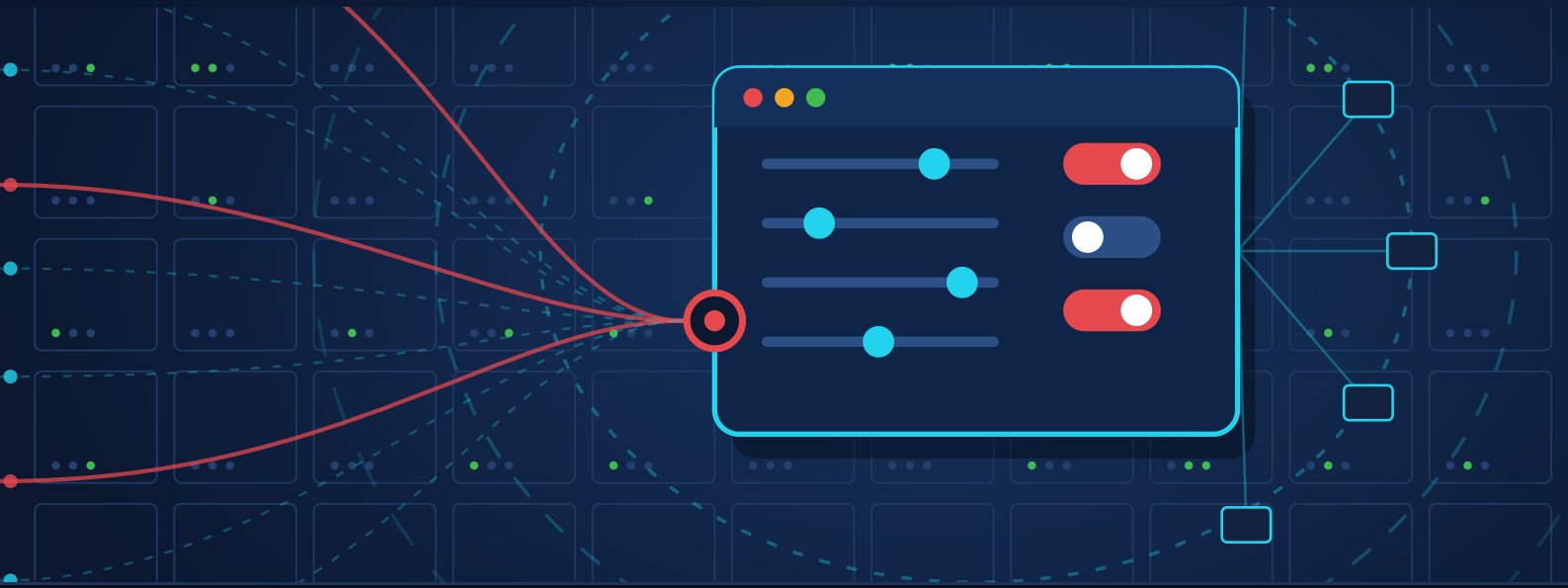
★ ★ ★ **Happy Veterans Day** · Thank you to all who served

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

The way in is the admin console

An exploited Barracuda chain on a three-day federal clock, an Outlook zero-day among about 1,094 Microsoft fixes, and a Xen Orchestra bypass that hands over whole hypervisor pools.

- **Barracuda ESG + 5 lines** exploited · KEV due 13 Nov
- **Xen Orchestra** auth bypass → root on XCP-ng
- **Fortinet**: ten criticals, some branches must migrate
- **Outlook CVE-2026-124194** leaks NTLMv2 hashes · exploited
- **Chrome zero-day**, BroadWorks, Openwave join KEV
- **NEAR AI & Fireworks AI** breached · Vanderbilt shut down



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 In the past 24 hours the confirmed or credible ways in were **a Barracuda admin UI, a Xen Orchestra console, FortiManager's FGFM port and an exposed AI inference server**. CISA gave agencies until **13 November** to fix the Barracuda pair and told them to look for compromise, not just patch. Microsoft's only exploited bug this month is a "Moderate" Outlook flaw. The common lesson: management planes that answer from the internet are being found and used.

The three actions that matter most today

1 **Barracuda: lock down admin UIs, patch, triage before 13 Nov**

Restrict admin interfaces to trusted networks, confirm each product's patch ID (ESG BNSF-40425/-40430, ADC/WAF BNADC-16586, BMA BNMA-32468, WCC BNWF-60060, WSG BNYF-24789) and review config-import/restore history on exposed devices. ↗ Barracuda ↗ CISA KEV

2 **Xen Orchestra: isolate, upgrade to 6.9.2 / 6.10.1, run Vates' host checks**

Block the eight published IPs and the onion C2. Any IOC hit means rotating every secret and reinstalling. ↗ Vates

3 **Microsoft and Chrome: Office fix, Exchange and DCs first, Chrome 157**

Ship the November Office update (CVE-2026-124194); Exchange servers and DCs in the first ring (CVE-2026-116928, -119958); force Chrome 157.0.8103.50/.51. ↗ MSRC ↗ ZDI ↗ The Hacker News

Story board

#	Story	Date label	Exploited?	Who should care
1	Barracuda ESG and appliance chain	KEV 10 Nov, due 13 Nov	YES	MSPs, SMB and school IT
2	Patch Tuesday: Outlook zero-day	10 Nov · KEV due 24 Nov	YES	Everyone; Exchange and AD first
3	Xen Orchestra VSA-2026-062	10 Nov	YES	MSPs, hosting, schools on XCP-ng
4	KEV: Chrome, BroadWorks, Openwave	KEV 10 Nov, due 24 Nov	YES	Endpoint fleets, telecom/UC
5	Fortinet's ten critical advisories	10 Nov (patched 21–22 Oct)	NO	Network engineers, MSPs
6	CopperDragon / Sparrow toolkit	10 Nov	YES	Telecom, government, MSPs
7	NEAR AI and Fireworks AI	9 Nov [72h]	YES	AI/ML teams, AI buyers
8	Vanderbilt shutdown, BYOD claim	9 Nov [72h]	INCIDENT	School, university, healthcare IT

Labels: CONFIRMED primary source · REPORTED secondary outlet · CLAIMED attacker or unverified · MAG212 ANALYSIS our judgement · UNKNOWN not established.

Small links ↗ like this cite sources. Diagrams are MAG212 originals; commands were **not tested** by us. KEV data: CISA GitHub mirror, catalog 2026.11.10 (cisa.gov and NVD CVSS not checked). Not opened: Mandiant MNDT pages, Cisco's BroadWorks advisory, Google's Chrome note, Notion's advisory, Vanderbilt's status page.

In this issue

01 **Barracuda's exploited chain gives root on six appliance lines** 4
KEV due 13 Nov · forensic triage

02 **Microsoft fixes an exploited Outlook hash leak** 5
About 1,094 CVEs · two zero-click 9.8s

03 **Xen Orchestra's empty-object cookie hands over XCP-ng hosts** 7
Vendor IOCs and host checks

04 **Chrome, BroadWorks and Openwave complete the KEV batch** 8
All due 24 Nov

05 **Fortinet's ten criticals: upgrade, or migrate** 9
FortiMail · FGFM · OSPF · FortiAuthenticator

06 **CopperDragon's Sparrow toolkit links three espionage campaigns** 11
Fake "certificate fix" lure

07 **AI inference platforms breached: NEAR AI and Fireworks AI** 12
SGLang RCE · LLMjacking

08 **Vanderbilt tells its campus to shut down devices** 13
BYOD gang claims the attack

◆ **Defender's Action Desk** 13
Checklist · KEV deadlines · pending items

◆ **Awareness lesson and briefly noted** 15
"A real certificate error never asks you to install a fix"

◆ **Source register** 16
78 sources, with whether we opened them

↻ Updates to yesterday's stories

- **Qubole: new detail.** REPORTED More than a dozen organisations were hit (yesterday: "multiple"). The campaign ran 14–26 October from a rented OVH server and Mullvad VPN, used TruffleHog to validate credentials and took S3 data, sometimes whole buckets. Wiz found a remotely bootable data-harvesting ISO but no evidence it was deployed; a separate 8–11 October wave tested customer-owned AWS keys. No actor named. Sentra's write-up is now out beside Wiz's; both carry IOCs. Yesterday's actions stand: audit vendor-trusting IAM roles, review CloudTrail from 1 October. [72h]
  ↗ SecurityWeek ↗ Sentra ↗ Wiz
- **France / IRGC fridge sabotage: still a pledge.** AP repeats Barrot's 9 November promise to seek sanctions "at the European level" and the Paris prosecutor's pursuit of arrest warrants. UNKNOWN No EU sanctions decision or G7 cyber statement found. ↗ Siasat/AP
- **Outlook zero-day, 10 Nov KEV additions and Fortinet** were only noted in yesterday's afternoon update; they now get full treatment in stories 2, 4 and 5. No new material found for sshole, SonicWall, Plex2Shell, Frontline or bee-js.

ACTIVELY EXPLOITED · MAIL & WEB GATEWAYS

01

Barracuda's exploited flaw chain gives attackers root on six appliance lines

Exploited | KEV due 13 Nov | Forensic triage | Advisory 2 Nov [72h] | Evidence: strong

CVES	AFFECTED	CONDITION	IOCS
CVE-2026-116606 (9.3) · CVE-2026-111560 (8.6)	ESG, Load Balancer ADC, BMA, WCC, WAF, WSG	Admin UI reachable; no credentials	None published

What happened

CONFIRMED Barracuda's advisory covers an authorization bypass in **Email Security Gateway only** (CVE-2026-116606, CVSS 9.3) and a command injection in **ESG, Load Balancer ADC, Message Archiver, WAF Control Center, WAF and Web Security Gateway** (CVE-2026-111560, CVSS 8.6). Chained, they give root. On 9 November at 21:00 EST Barracuda added that it had seen exploitation "affecting a small number of organizations". ↗ Barracuda CISA added both to KEV on **10 November**, due **13 November**, with **forensic triage "Yes"**, ransomware use "Unknown" and references to Mandiant disclosures MNDT-2026-0041/-0042. ↗ CISA KEV

REPORTED Previdian saw 17 attempts against CVE-2026-116606 from 15 IP addresses in three countries between 9 and 11 November; the IPs weren't published and the actors are unidentified. No ransomware link has been reported. ↗ SecurityWeek ↗ Previdian

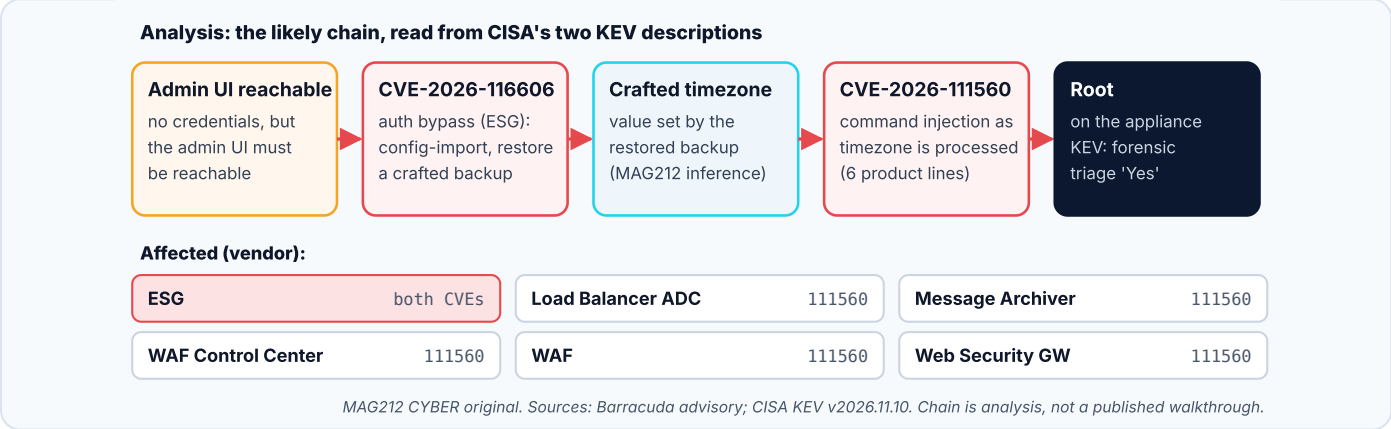


Figure 1 · The Barracuda chain, as MAG212 reads it. Two CVEs chained to root. The middle step is MAG212's inference from CISA's two KEV descriptions, not a published walkthrough. Below: the six affected product lines.
MAG212 CYBER original diagram, based on the Barracuda advisory and CISA KEV (10 Nov 2026).

Who is affected and how it works

Product	CVE(s)	Patch ID	Product	CVE(s)	Patch ID
ESG 9.4.017 and later	both	BNSF-40425	WAF Control Center	111560	BNWF-60060
ESG below 9.4.017	both	BNSF-40430	Web Application Firewall	111560	BNADC-16586
Load Balancer ADC	111560	BNADC-16586	Web Security Gateway	111560	BNYF-24789
Message Archiver	111560	BNMA-32468	Version thresholds given for ESG only	UNKNOWN	fixed firmware for the others

Source: Barracuda advisory.

CONFIRMED On 5 November Barracuda changed CVE-2026-116606's "Authentication Required" field to "No (Administrative UI Access Required)": no credentials, but the admin UI must be reachable. ↗ Barracuda KEV says the bypass lets an attacker invoke config-import and restore a crafted backup, and the injection runs root commands "when the crafted

timezone value is subsequently processed". ↗ CISA KEV MAG212 ANALYSIS That points to a crafted backup that sets a malicious timezone value. UNKNOWN Tooling, actors, start date and the Mandiant pages' contents.

What to look for

MAG212 ANALYSIS With no published IOCs: config-import or backup-restore events you didn't start, unexpected timezone changes, and admin-UI connections from outside your management networks.

Investigate, contain and remediate (in order)

1. **Restrict the admin UI now** to trusted networks; this is Barracuda's workaround. ↗ Barracuda
2. **Confirm the latest firmware and the patch ID** on every device. Devices several versions behind may need more than one update; apply manually if auto-patching didn't run. ↗ Barracuda Campus
3. **Triage before you trust a patched box.** MAG212 ANALYSIS Treat any appliance with an internet-reachable admin UI since 2 November as possibly compromised: preserve logs, review config history, involve Barracuda support or your IR provider.
4. MAG212 ANALYSIS If compromise is suspected, rotate LDAP bind, SMTP relay and admin credentials, and consider rebuilding rather than cleaning.

Verify recovery: the patch ID shows as applied on every device; the admin UI doesn't answer from an external vantage point; config history re-reviewed after patching. **Lesson** MAG212 ANALYSIS : MSPs should inventory admin-UI exposure across every client appliance this week.

PATCH TUESDAY · MICROSOFT 365, EXCHANGE, WINDOWS

02

Microsoft fixes an exploited Outlook hash leak among about 1,094 CVEs

1 exploited | KEV due 24 Nov | Two zero-click 9.8s | Published 10 Nov

ZERO-DAY	COUNT	CRITICAL	END OF SUPPORT
CVE-2026-124194 · Outlook · CVSS 6.5 Moderate	1,094 new (1,093 Microsoft-assigned)	63 (MAG212 count)	Windows 11 23H2 Ent/Edu: last month

What happened

CONFIRMED Of 1,342 entries in Microsoft's November data, **1,094 were first published on 10 November: 1,093 assigned by Microsoft and one by VulDB**. By MAG212's count of that data, 63 Microsoft-assigned CVEs are Critical. Exactly one is marked exploited and none publicly disclosed. ↗ MSRC REPORTED SecurityWeek also counts 1,094; ZDI says "about 1,090" and calls the count "a bit confusing". SecurityWeek notes 165 republished third-party CVEs (none from Chrome) and that this is the last month of updates for Windows 11 23H2 Enterprise and Education. ZDI counts 30 wormable CVEs by its own definition. ↗ SecurityWeek ↗ ZDI

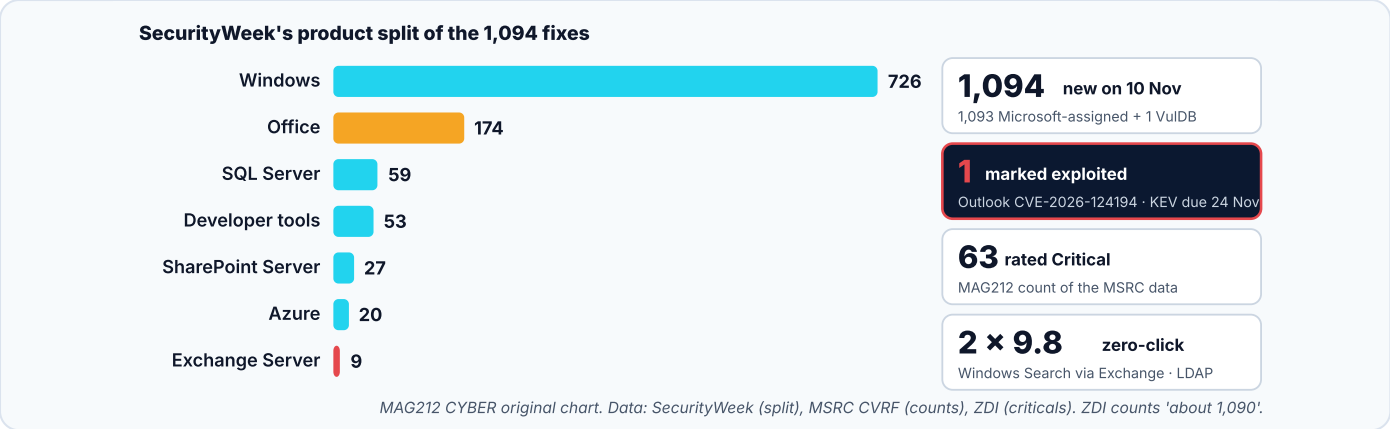


Figure 2 · November Patch Tuesday at a glance. SecurityWeek's product split, plus the counts that matter: one exploited CVE (a Moderate Outlook bug) and two unauthenticated 9.8 criticals.
MAG212 CYBER original chart. Data: SecurityWeek, MSRC CVRF (MAG212 count), ZDI.

The Outlook zero-day: who is affected and how it works

CONFIRMED CVE-2026-124194 is a spoofing flaw (missing warning before an unsafe action) in **Microsoft 365 Apps for Enterprise and Office LTSC 2021/2024**, rated "Exploitation Detected", customer action required. A user must **open a crafted message file**; Outlook then connects to an attacker-controlled location without the usual warning and **discloses the user's NTLMv2 hash**. The **Preview Pane is not an attack vector**. Credited to "nono" and Benoît Sevens. ↗ MSRC KEV: due 24 November, forensic triage "No". ↗ CISA KEV REPORTED ZDI says the hash could be used "to authenticate as the user". ↗ ZDI UNKNOWN Who exploited it, against whom, the delivery method and IOCs.

The criticals to patch next (per ZDI; none reported exploited)

CVE	Component	CVSS	Why it matters
CVE-2026-116928	Windows Search RCE, reached through **Exchange**	9.8	Crafted attachment triggers when the server indexes it; no user action
CVE-2026-119958	Windows LDAP RCE	9.8	No interaction; especially damaging on **domain controllers**
CVE-2026-119952	Windows Schannel RCE	8.1	"Exploitation More Likely" despite high complexity
CVE-2026-112967	Xbox Live Networking Service RCE	9.8	Unauthenticated heap overflow; ZDI sees real-world use as unlikely
CVE-2026-95962	Windows Virtual Filtering Platform RCE	n/a	Use-after-free from a crafted packet, no auth, race condition
CVE-2026-119990	Azure OpenAI elevation of privilege	9.8	Revised to **no customer action needed**

Source: ZDI. CVSS for CVE-2026-95962 was not captured.

Look for, contain and remediate (in order)

1. **Deploy the November Office updates** to Microsoft 365 Apps and Office LTSC 2021/2024. ↗ MSRC
2. **Patch Exchange servers and domain controllers first** for CVE-2026-116928 and CVE-2026-119958. ↗ ZDI
   MAG212 ANALYSIS Zero-click and unauthenticated, so expect exploit development.
3. MAG212 ANALYSIS Block outbound SMB/NTLM (TCP 445) to the internet and consider NTLM restrictions; review firewall logs for workstations, particularly Outlook, reaching internet hosts on 445.
4. MAG212 ANALYSIS Reset passwords for anyone who reports opening an odd message file and review their sign-ins.
5. **Plan Windows 11 23H2 Enterprise/Education migrations.** ↗ SecurityWeek

Verify recovery: patch reporting shows the November Office build on all Outlook clients and the November update on Exchange and DCs; outbound TCP 445 to the internet is blocked from inside. **Lesson** MAG212 ANALYSIS : this month's only exploited bug is "Moderate". Exploitation status should outrank CVSS, which is what KEV encodes.

ACTIVELY EXPLOITED · VIRTUALISATION

03

Xen Orchestra's empty-object cookie hands attackers root on XCP-ng hosts

Exploited | No CVE yet | Advisory 10 Nov | Evidence: strong (vendor, IOCs)

ADVISORY	FIXED	CVSS	LOGS
Vates VSA-2026-062 · Critical	XO 6.9.2 (stable) · 6.10.1 (latest)	Not available yet	Exploitation leaves none

What happened

CONFIRMED Vates rates VSA-2026-062, "Empty-object login token", Critical and says it is being actively exploited by an actor operating initially from `91.211.251.112:8001` and an onion address. There is no CVE yet. ↗ Vates REPORTED Credited to Filip Magic and Christoffer Olsen (TDC NET Security); THN adds that VirusTotal flags that IP as a RedLine Stealer C2. A crafted cookie, `authenticationToken=j:%7B%7D`, is parsed into an empty object that the token provider accepts, giving XO admin, then code execution on pools and root on hosts. ↗ The Hacker News UNKNOWN Start date and victim count.

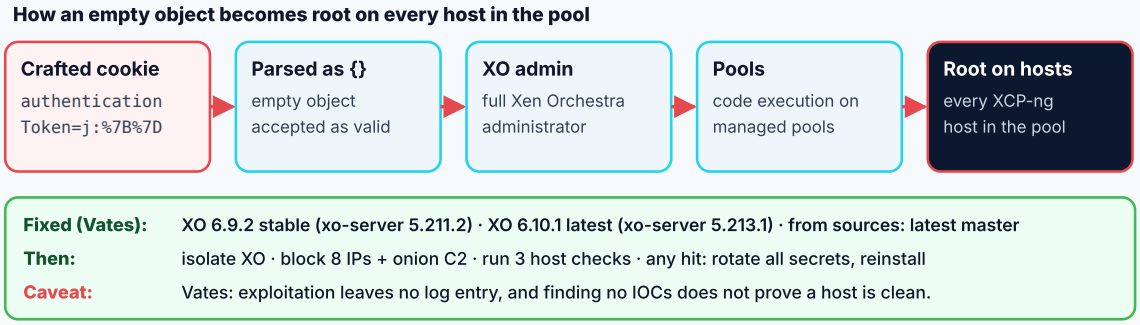


Figure 3 · From an empty cookie to root on XCP-ng. The reported bypass mechanics, with the vendor's fixed versions and response order. Exploitation leaves no logs.
MAG212 CYBER original diagram, based on Vates VSA-2026-062 and The Hacker News (10 Nov 2026).

Who is affected

Install type	Affected	Fixed (vendor)
Xen Orchestra, stable channel	before 6.9.2	**XO 6.9.2** (xo-server 5.211.2)
Xen Orchestra, latest channel	before 6.10.1	**XO 6.10.1** (xo-server 5.213.1)
Xen Orchestra Appliance (XOA)	yes	update to the versions above
From-sources builds	yes	latest master (PR #10748)

Source: Vates. **Conflict:** THN gives 6.9.1 / 6.10.0 with the same xo-server versions; we use the vendor's figures.

What to look for (vendor IOCs)

Type	Indicator (all from Vates VSA-2026-062)
Request pattern	`authenticationToken=j:%7B%7D` or `j:{}`
Host artifacts	a VM named `pivot2`; VMs with `hvm_serial: file`
Files	`/etc/cron.d/zz-ustar2`, `/etc/cron.d/zz-ustar`, `/.ustar5`, `/.ustar6`
IPs to block	`91.211.251.112` `193.148.56.72` `37.221.208.216` `45.66.35.11` `64.65.0.120` `64.65.62.160` `89.47.51.90` `92.60.37.247`

Type	Indicator (all from Vates VSA-2026-062)
Onion C2	`ustar3rqxgnskzgnwkgpofgtvxevm6cx3lxdbwt4mndtveqyaohid.onion:3333`

Vendor caveat: successful exploitation leaves no log entry, and finding no IOCs does not prove a host is clean. Vates

Host checks OS: XCP-ng (dom0) Shell: bash Privileges: root (MAG212 analysis; vendor doesn't state) READ-ONLY

```
# VMs whose platform settings include a file-backed serial port (IOC: hvm_serial: file)
xe vm-list params=name-label,platform | grep -B1 'hvm_serial: file'
# Search current and rotated xensource logs for file-backed serial configuration
zgrep -- '-serial file:' /var/log/xensource.log*
# Preload hijack and the published persistence files
ls -la /etc/ld.so.preload /.ustar* /etc/cron.d/zz-ustar*
```

Run on every XCP-ng host. Any output naming the IOCs above is a hit; "No such file" for the last command is the expected clean result. **Commands not tested by MAG212 CYBER**; copied from the Vates advisory.

Contain and remediate (in order, per Vates)

1. **Take XO off the internet** onto a dedicated management network; block the IPs and onion address.
2. **Upgrade** to XO 6.9.2 or 6.10.1 (xo-server 5.211.2 / 5.213.1); from-sources builds to latest master.
3. Optional interim WAF or reverse-proxy rule for the token patterns; Vates warns regex rules can be bypassed.
4. **Run the host checks** above on every host.
5. **If compromised:** rotate all secrets (proxy, backup remotes, root, pool secret, users, OTP, mail) and fully reinstall. ↗ Vates

Verify recovery: confirm the XO version, that the interface is unreachable from untrusted networks, re-run the checks, and confirm rotated secrets are in use. MAG212 ANALYSIS With no logs, reinstalling is the only high-confidence recovery for a host with any hit. Virtualisation control planes belong on an isolated network, especially for MSPs and schools that chose XCP-ng to save cost.

ACTIVELY EXPLOITED · BROWSERS & TELECOM

04

Chrome zero-day, Cisco BroadWorks and Openwave complete the 10 November KEV batch

Exploited | KEV 10 Nov · due 24 Nov | Evidence: medium–strong

Chrome CVE-2026-125350: exploited XML use-after-free

REPORTED Google is "aware that an exploit for CVE-2026-125350 exists in the wild". Reported anonymously on 6 November, it is the eighth exploited Chrome zero-day of 2026, fixed in **Chrome 157.0.8103.50/.51** (Windows, macOS) and **157.0.8103.50** (Linux). ↗ The Hacker News ↗ SecurityWeek CONFIRMED KEV notes it affects other Chromium browsers such as Edge and Opera. ↗ CISA KEV UNKNOWN Attack details, targets, IOCs, and whether Edge has shipped a fix; Google's release note was not opened. **Do** MAG212 ANALYSIS push 157.0.8103.50/.51 and force a browser restart, then track Edge and Opera. **Verify** the version in your endpoint inventory.

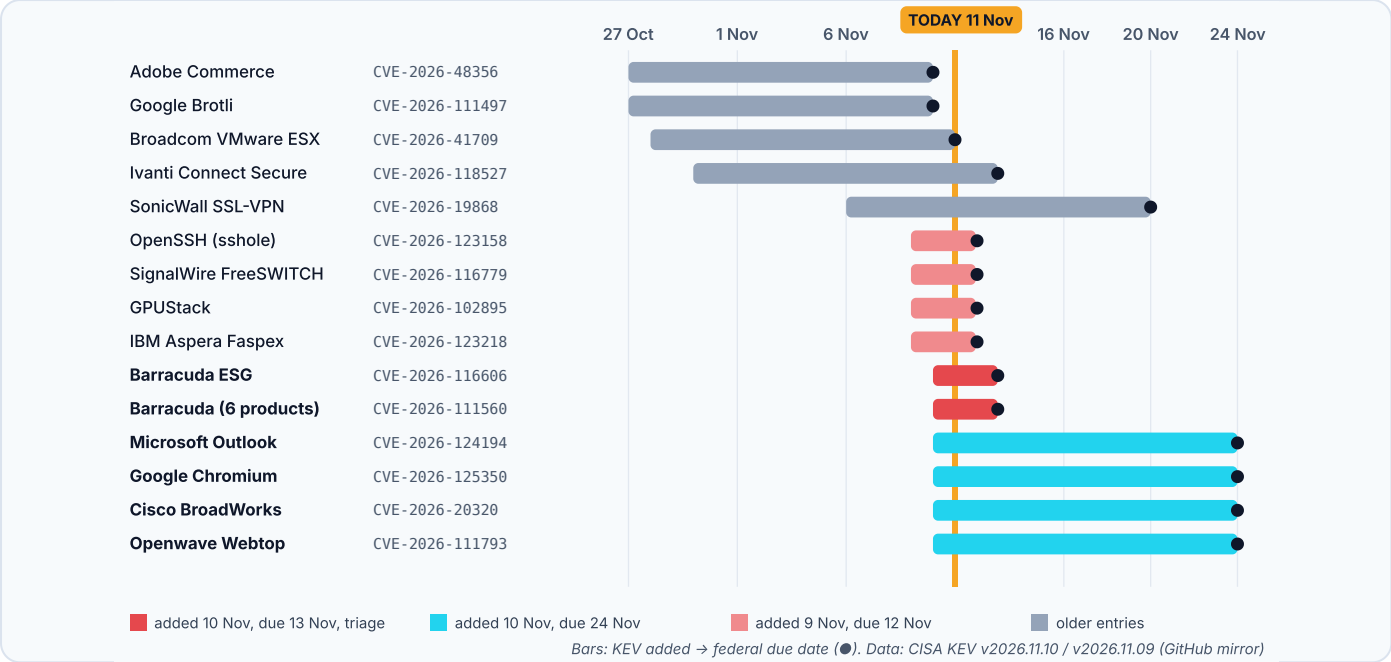


Figure 4 · KEV clocks running this week. Each bar runs from the date CISA added the flaw to KEV to the federal due date. The two Barracuda entries (red) have three days and a forensic-triage flag.
MAG212 CYBER original chart. Data: CISA KEV catalog v2026.11.10 and v2026.11.09 (GitHub mirror).

Cisco BroadWorks CVE-2026-20320: exploited XXE

CONFIRMED An XML external entity flaw that "could allow an unauthenticated, remote attacker to read sensitive configuration information"; due 24 November. ↗ CISA KEV UNKNOWN Fixed releases, CVSS and IOCs; read Cisco's advisory (not opened) before acting. MAG212 ANALYSIS Configuration can hold credentials, so plan rotation alongside the patch.

Openwave Webtop Media Transcoder CVE-2026-111793

CONFIRMED "Incorrect resource transfer between spheres" in Openwave Messaging Webtop Media Transcoder; due 24 November, referencing the vendor's GitHub advisory and JVN. ↗ CISA KEV ↗ Openwave UNKNOWN Versions and exploitation details. Narrow audience: telecom and messaging providers.

MAG212 ANALYSIS Where we recorded the flag, every three-day KEV deadline this week carries forensic triage "Yes" and every 14-day one "No": the short clock appears to signal suspected compromise, not just urgency.

CRITICAL, NOT YET EXPLOITED · NETWORK SECURITY

05

Fortinet's ten critical advisories: upgrade where you can, migrate where you can't

Known Exploited: No | No workarounds | Published 10 Nov · patched 21–22 Oct

What happened

CONFIRMED The FortiGuard PSIRT index grew from 324 to 370 advisories on 10 November. Every advisory page our researchers fetched says "Known Exploited: No" and offers no workaround, so upgrading is the only fix. ↗ FortiGuard ↗ Fortinet RSS REPORTED The fixes came from Fortinet's AI-assisted testing programme; watchTowr's Yordan Ganchev expects them to be "rapidly reverse-engineered, reproduced, and exploited" and advises restricting exposed management interfaces. ↗ Cybernews

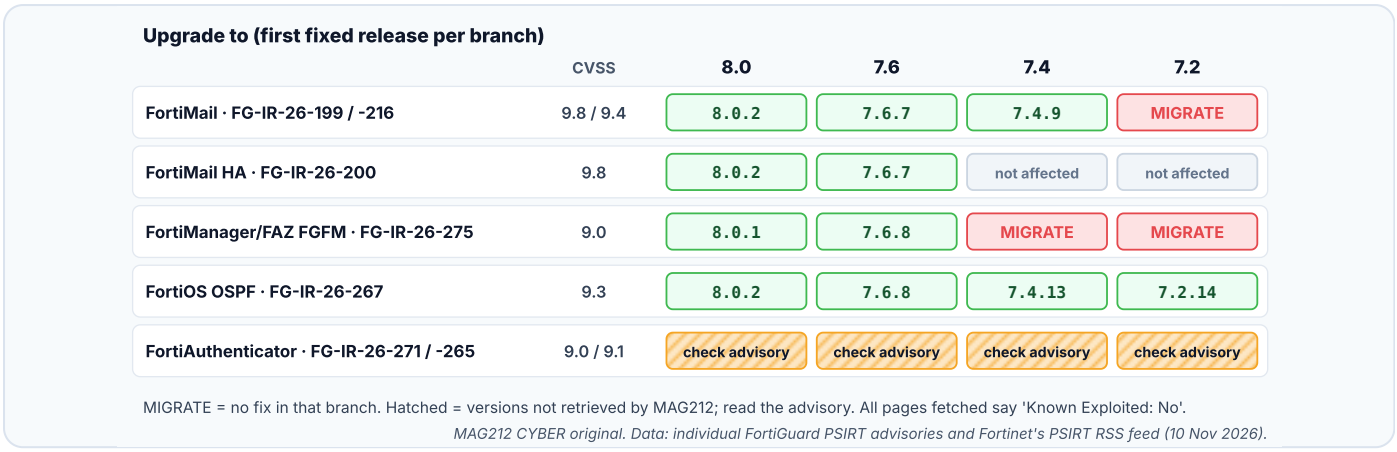


Figure 5 · Fortinet: where to upgrade, and where you must migrate. Fixed releases per branch from the advisories MAG212's researchers fetched. Red cells have no fix in-branch. FortiAuthenticator versions were not retrieved.
MAG212 CYBER original chart. Data: FortiGuard PSIRT advisories and RSS feed (10 Nov 2026).

Advisory	Product · CVE	Flaw (Fortinet summary)	CVSS	Fixed
FG-IR-26-199	FortiMail · CVE-2026-126147	Unauth path traversal → code execution	9.8	8.0.2 · 7.6.7 · 7.4.9 · 7.2 migrate · Cloud remediated
FG-IR-26-200	FortiMail · CVE-2026-126148	Unauth command injection via HA join-request packets	9.8	8.0.2 · 7.6.7 · 7.4/7.2 not affected
FG-IR-26-216	FortiMail · CVE-2026-126164	Unauth SQL injection → code execution*	9.4	as -199; 7.2 migrate
-207 / -208	FortiMail IBE	Unauth IBE session / recipient account takeover	9.1	not retrieved
FG-IR-26-275	FortiManager & FortiAnalyzer FGFM · CVE-2026-126261	Unauth code execution by anyone who can reach the FGFM port	9.0	8.0.1 · 7.6.8 · 7.4/7.2 migrate
FG-IR-26-267	FortiOS, FortiSASE OSPF · CVE-2026-126253	OSPF auth bypass; adjacent attacker may broadcast LSAs; PoC exists (E:P)	9.3	8.0.2 · 7.6.8 · 7.4.13 · 7.2.14; FortiSASE 26.3.2 (no action), 26.2–25.1 migrate
FG-IR-26-244	FortiManager/FAZ (+Cloud) · CVE-2026-126229	**Authenticated** admin reaches other VDOMs	9.1	not retrieved
FG-IR-26-271	FortiAuthenticator	Hard-coded password; credential bypass "in certain circumstances"	9.0	**check the advisory**
FG-IR-26-265	FortiAuthenticator	Incorrect authorization; authentication bypass	9.1	**check the advisory**

*FG-IR-26-216's Impact field says "Denial of service" while its summary describes code execution; treat it as the worse case. FortiAuthenticator advisories confirmed in Fortinet's RSS feed; MAG212 has not retrieved their affected or fixed versions. Earlier social-post figures for FortiManager are superseded by FG-IR-26-275.

Contain and remediate (in order)

1. MAG212 ANALYSIS Start with **FortiManager/FortiAnalyzer reachable on FGFM** from untrusted networks and **internet-facing FortiMail**: unauthenticated code execution, the class watchTowr expects to be weaponised.
2. **Schedule migrations now** for FortiMail 7.2 and FortiManager/FortiAnalyzer 7.4/7.2, which have no in-branch fix. ↗ FG-IR-26-199 ↗ FG-IR-26-275
3. Upgrade FortiOS for the OSPF flaw. MAG212 ANALYSIS Meanwhile, OSPF authentication and passive interfaces on user segments reduce adjacency exposure (general hardening, not Fortinet guidance).
4. Read FG-IR-26-271 and -265 for FortiAuthenticator versions and patch; it sits in front of VPN and admin MFA.
5. Restrict all management interfaces to trusted networks. ↗ Cybernews

Look for and verify: MAG212 ANALYSIS no IOCs exist; watch FGFM and FortiMail HA traffic from unexpected sources and OSPF neighbour changes you didn't make. Confirm firmware per device and, from outside, that FGFM and FortiMail admin/HA ports don't answer.

THREAT INTELLIGENCE · TELECOM & GOVERNMENT

06

CopperDragon's "Sparrow" toolkit ties three China-nexus espionage campaigns together

Active campaigns | Attribution assessed | Published 10 Nov | No CVEs

What happened

CONFIRMED After a year-long investigation, Check Point Research linked three clusters, **SilentDelivery, OceanGate and DarkWire**, through a shared framework it calls Sparrow, which it suggests is supplied by a developer it names **CopperDragon**. Targets: telecom providers, government, military, research and critical infrastructure in **21 countries**. CPR warns a telecom compromise could expose call records, subscriber locations, SMS and possibly lawful-intercept systems. ↗ Check Point ↗ Check Point Research

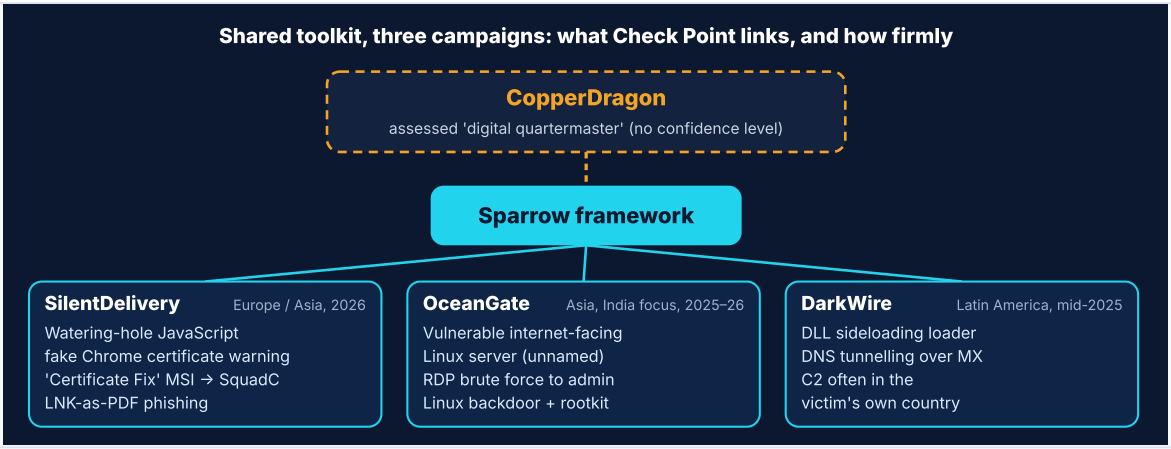


Figure 6 · One toolkit, three campaigns. Check Point links three clusters through the Sparrow framework. CopperDragon's role as supplier is assessed (dashed), with no formal confidence level.
MAG212 CYBER original diagram, based on Check Point Research and The Hacker News (10 Nov 2026).

How each cluster gets in

- **SilentDelivery** (Europe/Asia, 2026): obfuscated JavaScript on legitimate sites fingerprints visitors and shows a **fake Chrome certificate warning offering a "Certificate Fix"**, a trojanized MSI that drops a backdoor. Also LNK files disguised as PDFs sent to Indonesian organisations. ↗ The Hacker News
- **OceanGate** (2025–26, India focus): a "vulnerable internet-facing Linux server", with **no product or CVE named**, then RDP brute force to an admin account; Linux backdoors with an optional rootkit, Windows keylogger and credential stealers. ↗ The Hacker News
- **DarkWire** (mid-2025, Latin American telecom and government): DLL sideloading, DNS tunnelling over MX queries, C2 often in the victim's own country. ↗ The Hacker News ESET documented related Sparrow activity in Latin America in September. ↗ CSA

Attribution: assessed, not proven

REPORTED CopperDragon is "assessed" to supply FamousSparrow, Earth Estries, Tropic Trooper, UAT-9244 and UAT-8302; FamousSparrow's relationship to Salt Typhoon "remains unclear". ↗ The Hacker News CONFIRMED CPR's own caveat: shared malware or C2 "does not necessarily mean" the same actor, and it gives no formal confidence level. ↗ Check Point UNKNOWN No government corroboration found. We say "shared toolkit links three campaigns", not "one group".

What to look for, and what to do

CPR publishes domains, IP addresses and file hashes, plus host artifacts: a Run-key persistence value, a local account added to Administrators with remote token filtering disabled, custom firewall rules, distinctive C2 HTTP paths and a renamed LSASS dump. **We don't reprint the values: copy them verbatim from the Check Point Research report** into your tooling. Check Point's guidance, in order: ↗ Check Point

1. Sweep DNS, proxy and EDR telemetry for CPR's domains, IPs and hashes; hunt the host artifacts.

2. Treat any "certificate fix" or update utility as suspicious. MAG212 ANALYSIS Block unsigned MSIs from browser download folders.
3. Monitor for malicious DLL loading, credential dumping, keylogging and new persistence.
4. Restrict and monitor RDP, SMB and SSH, especially brute force on internet-facing hosts.
5. Inspect DNS, including tunnelling over MX, and unusual outbound traffic; inventory and patch internet-facing Linux servers.

Verify: MAG212 ANALYSIS after removal, the rogue account and firewall rules are gone and token-filtering policy is back to baseline; rotate credentials on any host with credential-dumping artifacts.

CONFIRMED BREACHES · AI PLATFORMS

07

AI inference platforms breached: NEAR AI via an SGLang RCE, Fireworks AI scope widens

Company-confirmed | 9 Nov [72h] · reported 10 Nov | No CVE, versions or IOCs

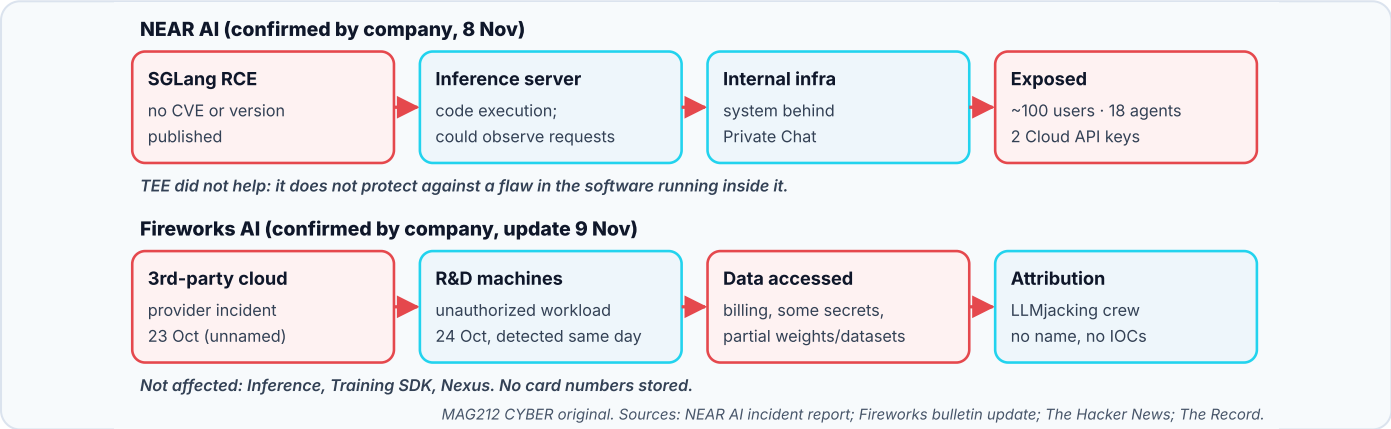


Figure 7 · Two AI platform breaches, two different routes. NEAR AI was entered through its inference engine; Fireworks through a third-party cloud provider. Neither has published a CVE, fixed version or IOC.
MAG212 CYBER original diagram, based on the NEAR AI and Fireworks AI disclosures (9 Nov 2026).

NEAR AI: an exploited SGLang flaw, and a TEE that didn't help

CONFIRMED On 8 November an attacker exploited an RCE in SGLang, "the open-source inference engine running on our servers", reached NEAR AI infrastructure and an internal system behind the deprecated Private Chat service. Exposed: names and emails of about 100 users (some with plan and balance data), chat history, settings and logs of 18 agents on a legacy deployment outside the TEE, and two Cloud customers' API keys (now revoked) that sat in logs. No sign stored Private Chat conversations were accessed, but the attacker "could also have observed user requests", including confidential-mode ones. NEAR AI revoked sessions and admin credentials, took Private Chat offline, patched every inference server, rotated credentials and notified users. ↗ NEAR AI REPORTED The TEE "does not protect against a vulnerability in the software running inside the environment". Brave's Leo uses a NEAR AI-run TEE; NEAR hasn't said whether the server handled Brave traffic. ↗ The Hacker News

UNKNOWN No CVE, endpoint, SGLang version or IOCs, and no SGLang advisory tied to the incident. CERT/CC listed six unpatched SGLang flaws in July, but **nothing links NEAR AI's breach to any of them**. **SGLang operators** (CERT/CC): keep SGLang off untrusted networks, segment it, set `SGLANG_USE_PICKLE_IPC=false` (a configuration change; restart the process, MAG212 analysis) and disable unused endpoints. ↗ CERT/CC MAG212 ANALYSIS Also require API keys and keep secrets out of inference-host logs.

Fireworks AI: an LLMjacking crew came in through a third-party cloud provider

CONFIRMED An unnamed cloud provider hosting Fireworks R&D machines had an incident on 23 October; on 24 October the attacker reached development machines and ran an unauthorized workload, detected the same day. Accessed: resource metadata, billing and shipping addresses, invoices, balances, secrets for a limited set of accounts and some

incomplete model weights and datasets. Not affected: Inference, Training SDK and Nexus; card numbers aren't stored. Fireworks attributes it to an unnamed, financially motivated group reselling tokens through illicit gateways (LLMjacking), engaged Unit 42 and told law enforcement. ↗ Fireworks REPORTED Affected accounts are a "limited number", all notified. The Record reports Notion was notified on 2 November, disconnected, disabled its Insights feature and stopped serving open-weight models via Fireworks. ↗ The Record **We do not report that Notion AI chats were exposed:** a THN headline says so, but neither its article body nor Fireworks' bulletin does, and we haven't read Notion's advisory. ↗ The Hacker News

Fireworks customers MAG212 ANALYSIS, FROM THE BULLETIN : rotate secrets stored in Fireworks and all API keys; look for keys you didn't create and odd usage or billing; treat uploaded datasets and fine-tunes as possibly exposed; alert on LLM usage spikes. **Lesson:** treat AI vendors as holders of your secrets, with scoped, rotatable keys on your third-party risk register.

INCIDENT · HIGHER EDUCATION

08

Vanderbilt tells its campus to shut down devices as the BYOD gang claims the attack

Ransomware "likely" (reported) | Announced 9 Nov [72h] | No 10–11 Nov update found



Figure 8 · What's confirmed, reported and claimed. Keep the three tiers apart: the university confirms an incident, officials reportedly say ransomware is likely, and the gang's numbers are unverified.
MAG212 CYBER original diagram. Sources: WSMV, The Record, Gizmodo, The Register.

CONFIRMED Vanderbilt has an active incident that may affect devices, systems and cloud services, and told users to "SHUT DOWN YOUR DEVICE IMMEDIATELY" and leave university Wi-Fi. It has about 14,000 students and more than 6,000 staff. ↗ WSMV ↗ The Record REPORTED Officials called it a "likely" ransomware attack; classes proceeded though some were cancelled; users reported ransom notes and files renamed with a `.byod` extension (Nashville Scene via Gizmodo, not officially confirmed). ↗ Gizmodo CLAIMED BYOD says it holds data on more than 1 million people including SSNs, plus the domain controller and research data. Vanderbilt didn't respond to Gizmodo. ↗ Gizmodo

REPORTED BYOD's first victim appeared on 29 September; it has also claimed Michigan State and UNM Health Sciences Center, which confirmed a "cybersecurity event" on 26 October. Its UNM machine count is unverified, as is a 9 November claim against the Texas Health and Human Services Commission. ↗ The Record ↗ The Register UNKNOWN Vector, official ransomware confirmation, restoration status and whether data was taken. No IOCs.

For school and university IT MAG212 ANALYSIS : (1) confirm tested offline or immutable backups of domain controllers and identity systems; (2) rehearse a campus-wide "shut down devices" message on a channel that works without email; (3) review privileged and domain-admin activity; (4) watch Vanderbilt's status page for a vector disclosure.

Defender's Action Desk

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

- ☐ NOW **Barracuda:** admin UI to trusted networks only; confirm patch IDs; review config-import/restore history; triage exposed boxes before 13 Nov. → 01

- [ ] **NOW** **Xen Orchestra:** isolate; XO 6.9.2 / 6.10.1; block 8 IPs + onion; run 3 host checks; any hit → rotate and reinstall. → 03
- [ ] **NOW** **Outlook and Chrome:** November Office update; Chrome 157.0.8103.50/.51 with forced restart. → 02 → 04
- [ ] **TODAY** **Exchange and DCs:** first ring for CVE-2026-116928 and CVE-2026-119958; block outbound TCP 445. → 02
- [ ] **TODAY** **Fortinet:** close FGFM and FortiMail exposure; book FortiMail 7.2 and FortiManager/FAZ 7.4/7.2 migrations. → 05
- [ ] **TODAY** **N-able on-prem N-central:** keep offline until the hotfix is verified (Briefly noted).
- [ ] **THIS WEEK** **AI vendors:** rotate Fireworks keys and secrets; keep SGLang off untrusted networks. → 07
- [ ] **THIS WEEK** **Hunting:** load CPR's CopperDragon IOCs; brief staff on fake "certificate fixes". → 06
- [ ] **THIS WEEK** **Git:** update to 2.56.1 or your branch's fix; no recursive clones of untrusted repos (Briefly noted).

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

CVE	Product	Added	Due	Triage
CVE-2026-48356 · -111497	Adobe Commerce · Google Brotli	27 Oct	10 Nov (passed)	—
CVE-2026-41709	Broadcom VMware ESX	28 Oct	**11 Nov (today)**	—
CVE-2026-123158 · -116779 · -102895 · -123218	OpenSSH · FreeSWITCH · GPUStack · IBM Aspera Faspex	9 Nov	**12 Nov**	Yes
CVE-2026-116606 · -111560	**Barracuda**	10 Nov	**13 Nov**	**Yes**
CVE-2026-118527	Ivanti Connect Secure	30 Oct	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	No

Bold: new in catalog 2026.11.10. "—" = flag not recorded in our notes. Ransomware use "Unknown" for every 10 Nov addition. Source: CISA KEV.

⏳ Pending at the cutoff: check before you act

- **Barracuda IOCs:** Mandiant's MNDT-2026-0041/-0042 pages, referenced by KEV, were not opened; no IOCs have been published. ↗ CISA KEV
- **Git for Windows:** no 2.56.1-based release as of 19:09 UTC on 10 Nov. ↗ The Hacker News
- **N-able N-central hotfix:** expected around midday 10 Nov; not confirmed. Check the N-able status page.
- **KEV 11 Nov additions:** none in the GitHub mirror at research time; cisa.gov not checked.
- **Also open:** FortiAuthenticator FG-IR-26-271/-265 and FG-IR-26-207/-208/-244 version tables; Cisco BroadWorks fixed releases; Edge/Opera status for CVE-2026-125350; Vanderbilt status updates.

Awareness lesson: "A real certificate error never asks you to install a fix"

For employees, teachers and students

CopperDragon's watering holes show a convincing fake Chrome certificate warning and offer a "Certificate Fix" download that is really espionage malware. ↗ The Hacker News

- Browsers **never** ask you to download software to fix a security warning.
- Close the tab and report it to IT.
- Don't open unexpected message-file attachments: opening one was enough to leak a password hash in this month's exploited Outlook flaw. ↗ MSRC

For leaders and owners

"If a management console can be reached from the internet, it is on someone's target list."

MAG212 ANALYSIS

Ask IT or your MSP for one page listing every management interface (appliances, hypervisors, RMM, AI/ML servers), whether it is internet-reachable, and who owns it.

Set a 30-day target of zero internet-exposed management planes.

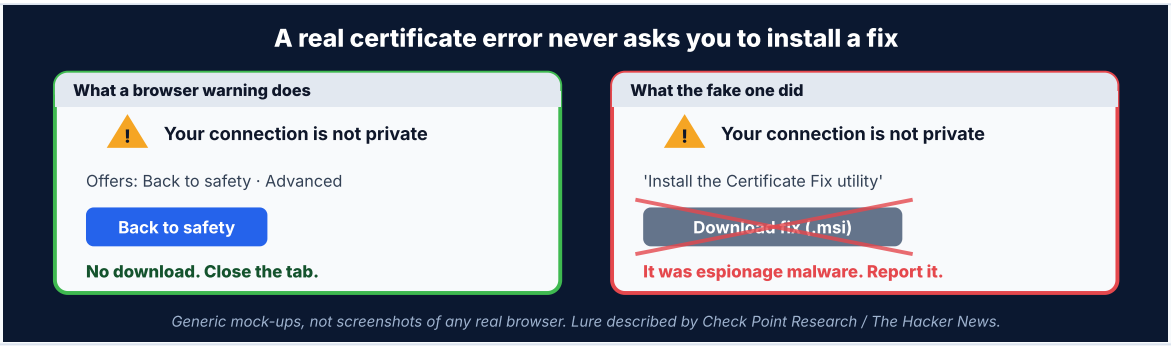


Figure 9 · Real warning versus fake 'fix'. Genuine browser warnings offer a way back, never a download. Generic mock-ups, not screenshots.

Conceptual MAG212 CYBER original illustration, based on the lure Check Point Research described.

Briefly noted

- **N-able N-central offline [72h].** REPORTED N-able took hosted N-central offline after a researcher posted more than 30 alleged zero-days with PoC code on 8 Nov (ISMG counts 33); N-able reports no evidence of exploitation and told on-prem customers to stay offline until patched. No CVEs yet. ↗ SecurityWeek ↗ GovInfoSecurity
- **Git CVE-2026-111760 (10 Nov).** CONFIRMED A malicious repo can swap a submodule's `.git` file for a symlink to hooks, running code on recursive clone. Fixed in Git 2.56.1, 2.55.1, 2.54.1, 2.53.1, 2.52.1, 2.51.3 and 2.50.2 and GHES 3.19.15/3.20.11/3.21.9/3.22.4; five more CVEs fixed. Not exploited. ↗ GitHub
  MAG212 ANALYSIS CI runners and AI coding agents cloning with `--recursive` are most at risk.
- **Adobe (10 Nov).** REPORTED About 110 flaws in nine products, none exploited; six Connect flaws score 10.0 and four AEM flaws 9.9. ↗ SecurityWeek
- **SAP (10 Nov).** REPORTED 42 notes (43 per Onapsis), nine critical, including ICM2SHELL and unauthenticated SAP Gateway RCE "ProxyGate"; not exploited. ↗ SecurityWeek
- **ICS Patch Tuesday (11 Nov).** REPORTED Siemens: 9 advisories, 10 flaws, two on Node2Shell exposure; Schneider, VDE CERT and Johnson Controls also published. ↗ 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. Links checked for form; not re-fetched at publication. Corrections: cyber.mag212.com.

1 CISA KEV catalog (GitHub mirror, v2026.11.10)
10 Nov 2026 · Primary (government) · Opened: Yes

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

3 Barracuda Campus: manual patch steps
n/a · Vendor documentation · Opened: Linked from advisory

4 SecurityWeek: Recently patched Barracuda vulnerabilities exploited
11 Nov 2026 · Secondary · Opened: Yes

5 Previdian: CVE-2026-116606
Nov 2026 · Researcher · Opened: Cited via SecurityWeek

6 BleepingComputer: Barracuda warns of critical flaws
3 Nov, updated 6 Nov 2026 · Secondary (background) · Opened: Yes

7 MSRC: CVE-2026-124194
10 Nov 2026 · Primary (vendor) · Opened: Yes (coordinator)

8 MSRC: November 2026 release notes / CVRF
10 Nov 2026 · Primary (vendor) · Opened: Yes (coordinator)

9 SecurityWeek: Exploited Outlook zero-day among 1,094 flaws
10 Nov 2026 · Secondary · Opened: Yes

10 ZDI: The November 2026 security update review
10 Nov 2026 · Researcher · Opened: Yes (table truncated)

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

12 The Hacker News: Hackers exploit critical Xen Orchestra flaw
10–11 Nov 2026 · Secondary · Opened: Yes

13 The Hacker News: Google issues Chrome security update
10 Nov 2026 · Secondary · Opened: Yes

14 SecurityWeek: Chrome update patches exploited XML zero-day
10 Nov 2026 · Secondary · Opened: Yes

15 Google Chrome Releases: stable channel update
10 Nov 2026 · Primary (vendor) · Opened: No

16 Cisco advisory cisco-sa-bworks-xxe-uwUd7CEt
Nov 2026 · Primary (vendor) · Opened: No

17 Openwave advisory CAN-2026-2032674
Nov 2026 · Primary (vendor) · Opened: No (KEV reference)

18 FortiGuard PSIRT index
10 Nov 2026 · Primary (vendor) · Opened: Yes

19 Fortinet PSIRT RSS feed
10 Nov 2026 · Primary (vendor) · Opened: Yes (coordinator)

20 FG-IR-26-199 (FortiMail)
10 Nov 2026 · Primary (vendor) · Opened: Yes

21 FG-IR-26-200 (FortiMail)
10 Nov 2026 · Primary (vendor) · Opened: Yes

22 FG-IR-26-216 (FortiMail)
10 Nov 2026 · Primary (vendor) · Opened: Yes

23 FG-IR-26-207 / -208 (FortiMail IBE) [2]
10 Nov 2026 · Primary (vendor) · Opened: RSS summary only

24 FG-IR-26-275 (FortiManager/FortiAnalyzer FGFM)
10 Nov 2026 · Primary (vendor) · Opened: Yes

25 FG-IR-26-267 (FortiOS/FortiSASE OSPF)
10 Nov 2026 · Primary (vendor) · Opened: Yes

26 FG-IR-26-244 (FortiManager/FortiAnalyzer dmserver)
10 Nov 2026 · Primary (vendor) · Opened: RSS/index only

27 FG-IR-26-271 / -265 (FortiAuthenticator) [2]
10 Nov 2026 · Primary (vendor) · Opened: RSS summary only

28 Cybernews: Fortinet critical flaws, November disclosure
Oct–Nov 2026 · Secondary (background) · Opened: Yes (yesterday)

29 Check Point Blog: CopperDragon
10 Nov 2026 · Primary (researcher) · Opened: Yes

30 Check Point Research: full CopperDragon report
10 Nov 2026 · Primary (researcher) · Opened: Yes (via summarising tool)

31 The Hacker News: Three China-nexus espionage campaigns linked through Sparrow
10 Nov 2026 · Secondary · Opened: Yes

32 CSA research note: FamousSparrow SparroWocky
Sep 2026 · Secondary (background) · Opened: Yes

33 NEAR AI: Security incident report (SGLang)
9 Nov 2026 · Primary (company) · Opened: Yes

34 NEAR AI on X: follow-up
Nov 2026 · Primary (company) · Opened: Cited via THN

35 The Hacker News: SGLang RCE exploit breaches NEAR AI
10 Nov 2026 · Secondary · Opened: Yes

36 Brave blog: browser AI E2EE
15 Oct 2026 · Background · Opened: Cited via THN

37 CERT/CC VU#281278 (SGLang)
30 Jul 2026 · Government CERT (background) · Opened: Yes

38 OSV: CVE-2026-15976
Modified 28 Oct 2026 · Database (background) · Opened: Yes

39 The Hacker News: SGLang CVE-2026-5760
Apr 2026 · Secondary (background) · Opened: Search result

40 Fireworks AI: October 2026 security incident update
9 Nov 2026 · Primary (company) · Opened: Yes

41 Fireworks AI: October 2026 security incident (original)
Oct 2026 · Primary (company) · Opened: Cited via THN/The Record

42 The Hacker News: Fireworks AI breach widens
10 Nov 2026 · Secondary · Opened: Yes

43 The Record: Fireworks says hackers stole data in October attacks
10 Nov 2026 · Secondary · Opened: Yes

44 Notion advisory: third-party AI vendor incident
Nov 2026 · Primary (company) · Opened: No

45 WSMV: Vanderbilt urges community to shut down devices
9 Nov 2026 · Secondary (local news) · Opened: Yes

46 The Record: Vanderbilt cyberattack ransomware alert
9–10 Nov 2026 · Secondary · Opened: Yes

47 Gizmodo: Attackers claim data on over 1 million Vanderbilt students and staff
9 Nov, modified 10 Nov 2026 · Secondary · Opened: Yes

48 ransomware.live: BYOD listing for Vanderbilt
Nov 2026 · Tertiary (leak-site tracker) · Opened: Cited via Gizmodo

49 Vanderbilt status page incident
Nov 2026 · Primary (university) · Opened: No

50 The Register: UNM HSC / BYOD
27 Oct 2026 · Secondary (background) · Opened: Yes

51 SecurityWeek: Over a dozen organizations hit in Qubole supply-chain attack
10 Nov 2026 (13:27 UTC) · Secondary · Opened: Yes

52 Sentra: Inside the Qubole supply-chain attack
Nov 2026 · Primary (researcher) · Opened: Cited via SecurityWeek

53 Wiz: Qubole cross-account access abused in the wild
~9 Nov 2026 · Primary (researcher) · Opened: Cited via SecurityWeek

54 Siasat/AP: France blames Iran, seeks European sanctions
10 Nov 2026 · Secondary (wire) · Opened: Yes

55 SecurityWeek/AP: France blames Iran for refrigerator cyberattack
10 Nov 2026 · Secondary (wire) · Opened: Yes (yesterday)

56 SecurityWeek: N-able takes N-central offline
10 Nov 2026 · Secondary · Opened: Yes

57 GovInfoSecurity: N-able takes platform offline after 33 zero-days
10 Nov 2026 · Secondary · Opened: Yes

58 Oracle-Security GitHub: N-Central 0-days
8 Nov 2026 · Researcher · Opened: Cited via SecurityWeek

59 N-able status page
Live · Primary (vendor) · Opened: No

60 GitHub blog: Git security vulnerabilities announced
10 Nov 2026 · Primary (vendor) · Opened: Yes

61 Git mailing list announcement
10 Nov 2026 · Primary (project) · Opened: Cited via GitHub

62 The Hacker News: Git patches flaw that lets malicious repos run code
10 Nov 2026 · Secondary · Opened: Yes

63 SecurityWeek: Adobe patches 110 vulnerabilities across 9 products
10 Nov 2026 · Secondary · Opened: Yes

64 SecurityWeek: SAP patches critical ICM2SHELL, ProxyGate
10 Nov 2026 · Secondary · Opened: Yes

65 SecurityWeek: ICS Patch Tuesday, Siemens flags Node2Shell exposure
11 Nov 2026 · Secondary · Opened: Yes

66 BleepingComputer: CISA warns of Node2Shell exploitation
Nov 2026 · Secondary (background) · Opened: Search result

67 SecurityWeek: CISA warns of Node2Shell exploitation
Nov 2026 · Secondary (background) · Opened: Search result

68 GCN: CISA Node.js deadline
Nov 2026 · Secondary (background) · Opened: Search result

69 CISA GovDelivery: ICSA-26-307-01
3 Nov 2026 · Primary (government, background) · Opened: Yes

70 SecurityWeek: IBM Aspera Faspex, SignalWire FreeSwitch exploited
Nov 2026 · Secondary · Opened: Yes

71 BleepingComputer: SonicWall SSL-VPN MFA bypass
6 Nov 2026 · Secondary (background) · Opened: Yes

72 BleepingComputer: French bank heist via service provider
7 Nov 2026 · Secondary (held, out of window) · Opened: Yes

73 Europol: investment-scam servers seized
3–4 Nov 2026 · Primary (government, held) · Opened: Yes

74 The Hacker News: Xen hypervisor flaws
10–11 Nov 2026 · Secondary · Opened: Headline only

75 The Hacker News: Microsoft Paint RCE fix
10–11 Nov 2026 · Secondary · Opened: Headline only

76 SecurityWeek: Bluetooth, AirPlay pairing flaws patched across Apple platforms
11 Nov 2026 · Secondary · Opened: Headline only

77 BleepingComputer homepage (Iris Ohyama item)
10–11 Nov 2026 · Secondary · Opened: Listing only

78 The Hacker News homepage
11 Nov 2026 · Secondary · Opened: Listing

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_2026-11-11