

MONTHLY CLIENT SECURITY BRIEF

{MSP name} Monthly Client
Security Brief — October 2026

Release baseline 2026-10-13 Intelligence / EPSS cutoff 2026-10-21 Edition 1

1,415

CVEs Microsoft first
published on 13 Oct

80

Microsoft October CVEs
rated Critical by Microsoft

1

Microsoft CVE marked
"Exploitation Detected"
this Patch Tuesday

24

CISA KEV additions in
October 2026 (catalog
2026.10.21)

10

Findings in this brief (9 P1,
1 P2)

P1 FIRST RESPONSE NOW §2.1 WHO HAS THIS EVERY WINDOWS PC

Windows Shell: Mark of the Web security feature
bypass

P1. Microsoft: "Exploitation Detected". CISA KEV added 2026-10-13. No ransomware campaign use reported (CISA: Unknown).

Microsoft: delivered as a crafted file by email or instant message.

CVE-2026-96951

MICROSOFT Important

CVSS 3.1 8.8 High

1.512% 74.24 pct

◆ KEV exploited

added 10-13 · due 10-16

ACCELERATED NEXT · THE OTHER P1 FINDINGS, MOST COMMON PRODUCT FIRST

Email gateways

§2.2 FortiMail · CVE-2026-104286

§2.3 Cisco Secure Email Gateway · CVE-2026-76519

Firewalls / VPN

§2.4 Ivanti Connect Secure · CVE-2026-104935

§2.5 PAN-OS · CVE-2026-0322

§2.6 Fortinet FortiOS/FortiProxy · CVE-2025-61624

Web servers

§2.7 PHP · CVE-2026-109618 / 109619

Remote support

§2.8 BeyondTrust Remote Support · CVE-2026-102764

Backup servers

§2.9 AhsayCBS · CVE-2026-105134 / 105133

EDITION

Release baseline	2026-10-13
EPSS cutoff	2026-10-21
Edition	1

KEY FACTS

CVEs Microsoft published 13 Oct	1,415
Microsoft Critical	80
Exploitation Detected	1
KEV additions Oct 1-21	24
...by 13 Oct	11
...14 to 21 Oct	13
Findings	10
P1 / P2	9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pct

EPSS: probability; bar = percentile rank

KEY exploited

KEV: catalog evidence of exploitation

{MSP name} Monthly Client Security Brief: October 2026

Data checked 21 Oct 2026, 22:27-22:29 UTC. Informational only; see the note at the end.

FORWARD TO CLIENTS

Part 1. Client note (forward or paste as-is)

What happened this month. On 13 October, Microsoft released its monthly Windows and Office updates. One of the Windows problems fixed was already being used by attackers, according to Microsoft and the US Cybersecurity and Infrastructure Security Agency (CISA). It lets a harmful file sent by email or chat get past the warning Windows normally shows before you open something downloaded from the internet. Separately, CISA added several remote-access, email-filtering and backup products to its list of flaws attackers are using.

Who is likely affected. Any business with Windows PCs. Also any office running Windows 11 Home or Pro, version 24H2: Microsoft lists 13 October 2026 as the end of updates for that version, so those PCs need to move to a newer version to keep getting security fixes.

One thing for staff to do this week. If you get a file or link you weren't expecting, even from someone you know, check with the sender by phone or a separate message before you open it. Don't count on Windows to warn you.

What {MSP name} is doing: [MSP: describe only what you have actually done, e.g. "We are installing the October updates on all managed PCs."]

Part 2. Patch-first list for the technical team

Scope. This covers Microsoft's 13 Oct 2026 release and the CISA KEV additions from 1 to 21 Oct.

- Microsoft: 1,415 CVEs first published on 13 Oct, per its data as of the 21 Oct revision (1,407 of them assigned by Microsoft as CNA, 8 by other CNAs). Microsoft rated 80 of them Critical, marked 1 exploited and 2 publicly disclosed.
- By CVSS (each CVE's highest score in Microsoft's data), the same 1,415 split into 62 Critical, 987 High, 362 Medium and 4 unscored. Microsoft's own Critical rating (80) and the CVSS Critical band (62) measure different things.
- CISA KEV: 24 additions (11 by 13 Oct, 13 from 14 to 21 Oct).

Below are the **10 findings to act on first**: nine from the Microsoft release and the KEV additions, plus one PHP finding (\$2.7). The PHP item is **not part of Patch Tuesday**: it comes from the PHP project's 21 Oct advisories and Ubuntu. This is not a full patch list, and it is not tied to your clients' assets: a finding applies only where the product is actually deployed.

Priority bands: editorial recommendations, not Microsoft or CISA deadlines.

- **P1 First response (24-72h):** applicable KEV exposure or credible compromise evidence.
- **P2 Accelerated (7 days):** reachable remote code execution, untrusted mail or content processing, or high-impact identity or management services.
- **P3 Standard high (14 days):** High/Critical with constrained paths or prerequisites.
- **P4 Remaining cycle:** other applicable updates.

How to read a card. Each card opens with a signal row: CVE, the vendor's own rating, CVSS, EPSS and KEV status.

- **Order:** priority band first. Inside P1, cards are grouped by how many clients are likely to run the product (our editorial judgement): Windows, then email gateways, firewalls/VPN, web servers, remote support and backup servers. Within a group, the order is CVSS base score, then exploitation evidence, then EPSS.
- **Who has this:** a neutral tag naming the kind of client system the product runs on. It is editorial and not based on your asset data.

EDITION	
Release baseline	2026-10-13
EPSS cutoff	2026-10-21
Edition	1
KEY FACTS	
CVEs Microsoft published 13 Oct	1,415
Microsoft Critical	80
Exploitation Detected	1
KEV additions Oct 1-21	24
...by 13 Oct	11
...14 to 21 Oct	13
Findings	10
P1 / P2	9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pctl

EPSS: probability; bar = percentile rank

KEV exploited

KEV: catalog evidence of exploitation

- **CVSS:** the vendor's (CNA's) score in its newest version. Bands: Critical 9.0–10.0, High 7.0–8.9, Medium 4.0–6.9. Scores from CVSS 3.1 and 4.0 are not strictly comparable. A vendor rating such as Microsoft "Important" is not a CVSS band.
 - **EPSS:** FIRST's estimate of the probability that a CVE will be exploited in the wild in the next 30 days, given as a percentage with its percentile. All scores are dated 2026-10-21. EPSS can lag on brand-new CVEs, and a low EPSS never outweighs confirmed exploitation.
 - **KEY:** "added" and "due" are CISA catalog dates. The due dates are set under CISA's federal directive (BOD 26-04) and are not private-sector deadlines. A ransomware value of "Unknown" does not mean none.
 - **Vendor fact vs. our advice:** a vendor name marks a fact from that vendor's advisory. "General measure" and "general check" mark our own advice.
- Fixing is not recovering.** Installing a fix closes the hole. It does not by itself prove a system was never compromised, or remove anything an attacker already left behind. For internet-facing appliances that were exposed before patching, follow the vendor's investigation guidance, linked in each card.

P1 First response (24–72h)

P1 First response

WHO HAS THIS Every Windows PC

§2.1

Windows Shell: Mark of the Web security feature bypass

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEY / EXPLOITATION
CVE-2026-96951	MICROSOFT Important	8.8 High CVSS 3.1	1.512% 74.24 pctl · scored 2026-10-21	KEY exploited added 10-13 · due 10-16

PRIORITY P1. Microsoft: "Exploitation Detected". CISA KEV added 2026-10-13. No ransomware campaign use reported (CISA: Unknown).

EXPOSURE AND IMPACT Command injection in Windows Shell that lets a crafted file evade Mark of the Web (MOTW) defenses, i.e. the "downloaded from the internet" warning. Microsoft: delivered as a crafted file by email or instant message. No privileges needed, but the vector requires **user interaction**: the user has to open the file. MSRC lists Windows 10, Windows 11 and Windows Server 2012 R2 through 2025.

PERMANENT REMEDIATION October 13 security update; Microsoft says a restart is required.

WINDOWS VERSION	FIXED IN
Win 11 24H2 / 25H2 / 26H2	KB5127648 builds 26100 / 26200 / 26300.9711
Win 11 26H1	KB5127646 build 28000.3231
Win 11 23H2	KB5126653 build 22631.7652
Win 10 21H2 / 22H2	KB5126657 builds 19044 / 19045.7807
Win 10 1809 / Server 2019	KB5126651 build 17763.9376
1607 / Server 2016	KB5126868 build 14393.9612
Server 2022	KB5126655 build 20348.5761
Server 2025	KB5126646 build 26100.33650

EDITION

Release baseline	2026-10-13
EPSS cutoff	2026-10-21
Edition	1

KEY FACTS

CVEs Microsoft published 13 Oct	1,415
Microsoft Critical	80
Exploitation Detected	1
KEV additions Oct 1-21	24
...by 13 Oct	11
...14 to 21 Oct	13
Findings	10
P1 / P2	9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pctl

EPSS: probability; bar = percentile rank

KEV exploited

KEV: catalog evidence of exploitation

§2.1 WINDOWS SHELL · CONTINUED

WINDOWS VERSION	FIXED IN
Server 2012 R2	KB5126836 build 6.3.9600.23470

Outlook.com is also listed, as a service-side release (20260925.100); that does not replace patching Windows.

TEMPORARY EXPOSURE REDUCTION	No vendor workaround published; patch is the fix. (Microsoft lists no workaround or mitigation.) General measures (not a fix): attachment filtering and application control may reduce opportunity while you deploy; the Part 1 staff tip covers the user side.
VALIDATION	After the restart, confirm the OS build is at or above the fixed build (e.g. winver shows 26100.9711 or later on 24H2); a later cumulative update also counts (general check). Microsoft's KB5127648 known issues: Smart App Control may not turn back on if it was off; non-admin Remote Desktop to hosts with Administrator protection may fail; NTLMv1 SSO now defaults to blocked, which may affect MS-CHAPv2 Wi-Fi/VPN. KB5127648 is the last update for Windows 11 24H2 Home and Pro.
REFERENCES	MSRC CVE-2026-96951 · KB5127648 · evulnable CVE-2026-96951

P1 First response WHO HAS THIS Email gateways

§2.2

Fortinet FortiMail: unauthenticated arbitrary file write

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2026-104286	FORTINET Critical	9.8 Critical CVSS 3.1	2.201% 82.36 pctl · scored 2026-10-21	KEV exploited added 10-01 · due 10-04

PRIORITY	P1. Fortinet: "reported to be exploited in the wild". CISA KEV added 2026-10-01. No ransomware campaign use reported (CISA: Unknown).										
EXPOSURE AND IMPACT	Path traversal plus a NULL-byte flaw. Fortinet: an unauthenticated attacker can write arbitrary files on the underlying system with crafted HTTP/HTTPS requests; no user interaction. Fortinet's workaround points to the IBE (encryption) feature and the webmail interface. The impact is on the mail security appliance.										
PERMANENT REMEDIATION	<table><tr><th>FORTIMAIL BRANCH</th><th>FIXED IN</th></tr><tr><td>8.0.0-8.0.1</td><td>8.0.2+</td></tr><tr><td>7.6.0-7.6.6</td><td>7.6.7+</td></tr><tr><td>7.4.0-7.4.8</td><td>7.4.9+</td></tr><tr><td>7.2.0-7.2.9</td><td>Upgrade to the 7.4 branch or later</td></tr></table> Fortinet updated FortiMail Cloud on 5 Oct 2026.	FORTIMAIL BRANCH	FIXED IN	8.0.0-8.0.1	8.0.2+	7.6.0-7.6.6	7.6.7+	7.4.0-7.4.8	7.4.9+	7.2.0-7.2.9	Upgrade to the 7.4 branch or later
FORTIMAIL BRANCH	FIXED IN										
8.0.0-8.0.1	8.0.2+										
7.6.0-7.6.6	7.6.7+										
7.4.0-7.4.8	7.4.9+										
7.2.0-7.2.9	Upgrade to the 7.4 branch or later										
TEMPORARY EXPOSURE REDUCTION	Vendor workaround (Fortinet): turn off IBE (GUI: Encryption > IBE > IBE Service off; CLI: config system encryption ibe, set status disable, end). Or block webmail from the internet, or limit it to trusted private networks. Or, with a WAF in front, block POST requests to /ibe that contain ../.										
VALIDATION	Confirm the firmware version is at or above the fixed release (general check). If the workaround is used, confirm IBE shows disabled. Fortinet lists indicators of compromise (IPs and log entries); review logs against them, because patching does not remove an existing compromise.										
REFERENCES	Fortinet FG-IR-26-175 · evulnable CVE-2026-104286										

EDITION

Release baseline2026-10-13

EPSS cutoff2026-10-21

Edition1

KEY FACTS

CVEs Microsoft published1,415

Microsoft Critical80

Exploitation Detected1

KEV additions Oct 1-2124

...by 13 Oct11

...14 to 21 Oct13

Findings10

P1 / P29 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512%74.24 pctl

EPSS: probability; bar = percentile rank

KEV exploited

KEV: catalog evidence of exploitation

P1 First responseWHO HAS THISEmail gateways§2.3

Cisco Secure Email Gateway: arbitrary file write via email attachment

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2026-76519	CISCO Critical	9.8 Critical CVSS 3.1	1.573% 75.19 pctl · scored 2026-10-21	KEV exploited added 10-14 · due 10-17

PRIORITY

P1. Cisco: became aware of active exploitation in October 2026. CISA KEV added 2026-10-14. No ransomware campaign use reported (CISA: Unknown).

EXPOSURE AND IMPACT

Cisco: an **unauthenticated, remote** attacker sends an email with a crafted attachment through the gateway; no user click is needed. A successful attack can write files and run commands as root. Only affected when the File Reputation service (Cisco AMP) is on for a mail policy and Content Scanner Tools is older than 25.3.0.5525.

PERMANENT REMEDIATION

Content Scanner Tools 25.3.0.5525 or later (delivered to supported releases; no restart; automatic when auto-updates are on). Or AsyncOS **15.5.5-014** (15.5) or **16.5.0-780** (16.5). For 16.0, migrate to a fixed release (Cisco).

TEMPORARY EXPOSURE REDUCTION

Cisco: "There are no workarounds that address this vulnerability." Patch is the fix. Cisco's general hardening advice (not a fix): block internet access to the appliance, or limit it to known, trusted hosts.

VALIDATION

Run `contentscannerstatus` at the CLI and confirm Content Scanner Tools is 25.3.0.5525 or later (Cisco). Cisco also describes a `system_logs` check for attempted exploitation. If exploitation is suspected: for physical appliances, contact Cisco TAC. For virtual ones, record forensic data first (Cisco says upgrading a compromised instance destroys logs), deploy a fresh fixed VM, rebuild the configuration and renew credentials. Restore every member of an affected cluster.

REFERENCES

[Cisco cisco-sa-esa-afw-zqYJkxp · evulnable CVE-2026-76519](#)

P1 First responseWHO HAS THISFirewalls / VPN§2.4

Ivanti Connect Secure (VPN): authentication bypass to command execution

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2026-104935	IVANTI High	8.6 High CVSS 3.1	25.982% 97.98 pctl · scored 2026-10-21	KEV exploited added 10-13 · due 10-16

PRIORITY

P1. Ivanti: "aware of exploitation in the wild affecting a limited number of customers at the time of disclosure". CISA KEV added 2026-10-13. No ransomware campaign use reported (CISA: Unknown).

EXPOSURE AND IMPACT

Authentication bypass by spoofing. Ivanti: a **remote, unauthenticated** attacker can run arbitrary commands; no user interaction. VPN gateways face the internet by design.

PERMANENT REMEDIATION

ICS **25.1.1.2, 25.1.3.0 / 25.1.3.1, or 22.8R2.5** (Ivanti). Affected: 25.1.1.1 and earlier, 25.1.2.2 and earlier, 22.8R2.4 and earlier. 22.7R2.14 and earlier are not affected. 25.1.3.0 needs the ISA4500/6500/8500 platform.

TEMPORARY EXPOSURE REDUCTION

No vendor workaround published; patch is the fix.

EDITION	
Release baseline	2026-10-13
EPSS cutoff	2026-10-21
Edition	1

KEY FACTS	
CVEs Microsoft published 13 Oct	1,415
Microsoft Critical	89
Exploitation Detected	1
KEV additions Oct 1-21	24
...by 13 Oct	11
...14 to 21 Oct	13
Findings	10
P1 / P2	9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pctl

EPSS: probability; bar = percentile rank

KEV exploited

KEV: catalog evidence of exploitation

§2.4 IVANTI CONNECT SECURE (VPN) · CONTINUED

VALIDATION	Confirm the ICS version is one of the resolved releases (general check). Ivanti recommends running its Integrity Checker Tool regularly, and following its recovery steps if exploitation is suspected. Patching alone does not prove the appliance was not compromised.
REFERENCES	Ivanti advisory · evulnable CVE-2026-104935

P1 First response

WHO HAS THIS Firewalls / VPN

§2.5

Palo Alto Networks PAN-OS: authenticated RCE in the management interface

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2026-0322	PALO ALTO High (urgency Highest)	8.6 High CVSS 4.0	1.215% 68.31 pctl · scored 2026-10-21	KEV exploited added 10-14 · due 10-17

PRIORITY	P1. Palo Alto: "Very limited exploitation has been observed targeting the Palo Alto Networks management interface". CISA KEV added 2026-10-14. No ransomware campaign use reported (CISA: Unknown).
EXPOSURE AND IMPACT	Code injection in the PAN-OS management interface (PA-Series, VM-Series and Panorama). Palo Alto: an authenticated attacker with network access to the management interface can run code as root (CVSS: high privileges); no user interaction. Palo Alto says risk is highest when the management interface is reachable from the internet. Cloud NGFW and Prisma Access are not affected.

PERMANENT REMEDIATION	BRANCH	FIXED IN
	12.2	12.2.4
	12.1	12.1.10-h2 or 12.1.7-h8 / 12.1.4-h12
	11.2	11.2.16 or 11.2.13-h3 / 11.2.10-h15 / 11.2.7-h21 / 11.2.4-h22
	11.1	11.1.16-h3 or 11.1.13-h15 / 11.1.10-h35 / 11.1.7-h11 / 11.1.6-h39 / 11.1.4-h37
	10.2	10.2.18-h12 or 10.2.16-h11 / 10.2.13-h26 / 10.2.10-h41 / 10.2.7-h38

Older, unsupported versions: upgrade to a supported fixed version.

TEMPORARY EXPOSURE REDUCTION	Palo Alto: "No known workarounds exist." Vendor-described risk reduction (not a fix): allow management access only from trusted internal IPs or a single jump box. Threat Prevention customers can also enable Threat IDs 510046 and 510047 (content 9159-10287 or later); this gives limited coverage and needs SSL decryption of management traffic.
VALIDATION	Confirm the PAN-OS version is at or above the fixed release for its branch, and that the management interface is not reachable from the internet (general check).
REFERENCES	Palo Alto CVE-2026-0322 · evulnable CVE-2026-0322

EDITION

Release baseline 2026-10-13
EPSS cutoff 2026-10-21
Edition 1

KEY FACTS

CVEs Microsoft published 13 Oct 1,415
Microsoft Critical 80
Exploitation Detected 1
KEV additions Oct 1-21 24
...by 13 Oct 11
...14 to 21 Oct 13
Findings 10
P1 / P2 9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pctI

EPSS: probability; bar = percentile rank

KEY exploited

KEV: catalog evidence of exploitation

P1 First response

WHO HAS THIS Firewalls / VPN

§2.6

Fortinet FortiOS / FortiProxy / FortiPAM / FortiSwitchManager: CLI path traversal

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2025-61624	FORTINET Medium	6.0 Medium CVSS 3.1	1.081% 64.80 pctI · scored 2026-10-21	KEY exploited added 10-16 · due 10-19

PRIORITY P1 because it is in KEV (added 2026-10-16) and Fortinet lists "Known Exploited: Yes". It sits last among firewalls/VPN because it needs an admin account. CVSS 6.0 is from Fortinet's advisory; Fortinet's CVE record lists 5.4. Both are Medium. No ransomware campaign use reported (CISA: Unknown).

EXPOSURE AND IMPACT Path traversal in the command-line interpreter. Needs an **authenticated, privileged** attacker: CISA says an admin profile with at least read-write permissions. The attacker can then write or delete arbitrary files with crafted CLI commands. No user interaction.

PERMANENT REMEDIATION	BRANCH	FIXED IN
	FortiOS 7.6	7.6.5+
	FortiOS 7.4	7.4.10+
	FortiProxy 7.6	7.6.5+
	FortiProxy 7.4	7.4.12+
	FortiPAM	1.7.1+
	FortiSwitchManager 7.2	7.2.8+
	FortiSwitchManager 7.0	7.0.7+
	FortiOS 7.2 / 7.0 / 6.4	Migrate to a fixed release Fortinet names no version
	FortiProxy 7.2 / 7.0	Migrate to a fixed release Fortinet names no version
	FortiPAM 1.0-1.6	Migrate to a fixed release Fortinet names no version

Fortinet first published this advisory on 14 Apr 2026.

TEMPORARY EXPOSURE REDUCTION Vendor-supported (Fortinet): FortiGuard virtual patch "FG-VD-59270.0day" in FMWP database update 25.120. General measure (not a fix): review admin accounts and limit read-write admin access.

VALIDATION Confirm the firmware version is at or above the fixed release (general check).

REFERENCES [Fortinet FG-IR-26-122](#) · [evulnable CVE-2025-61624](#)

EDITION

Release baseline	2026-10-13
EPSS cutoff	2026-10-21
Edition	1

KEY FACTS

CVEs Microsoft published 13 Oct	1,415
Microsoft Critical	89
Exploitation Detected	1
KEV additions Oct 1-21	24
...by 13 Oct	11
...14 to 21 Oct	13
Findings	10
P1 / P2	9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pctl

EPSS: probability; bar = percentile rank

KEV exploited

KEV: catalog evidence of exploitation

P1 First response

WHO HAS THIS Web servers

§2.7

PHP (web servers): two unauthenticated remote code execution flaws

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2026-109618	PHP Critical	9.2 Critical CVSS 4.0	No EPSS score yet	Not in KEV
CVE-2026-109619	PHP Critical	9.2 Critical CVSS 4.0	No EPSS score yet	Not in KEV

PRIORITY

P1 is an editorial call based on third-party exploitation reports. watchTower: "Exploitation has been observed in the wild as of the 21st of October through watchTower's Attacker Eye global honeypot network." Cloudflare: it "observed attack traffic targeting our customers" and says the flaws leaked before the official release date. Neither CVE is in CISA KEV (catalog 2026.10.21, checked 2026-10-22 00:36 UTC). CISA's SSVCC entry in the CVE records lists exploitation as "none", and PHP's own advisories make no in-the-wild claim. If you discount the watchTower and Cloudflare reports, it is still at least P2 (reachable unauthenticated RCE). **Not part of Microsoft Patch Tuesday:** disclosed and fixed by the PHP project on 21 Oct 2026. FIRST EPSS has no score yet, and EPSS can lag on new CVEs. NVD separately scores both CVSS 3.1 9.8 Critical.

EXPOSURE AND IMPACT

PHP: **unauthenticated** remote code execution as the web worker account; no login or user interaction needed (CVSS vector: AC:H/AT:P, PR:N/UI:N).

- **109618:** out-of-memory handling can interrupt PHP while request data is only partly set up, and cleanup then treats that half-built data as valid.
- **109619:** request state can survive after its memory is freed and be reused by a later request on the same worker. PHP says this can also disclose heap memory.

php.net: at risk are "all PHP installations serving web requests, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed", with the risk highest for mod_php. Affected per PHP: 8.2 before 8.2.35, 8.3 before 8.3.36, 8.4 before 8.4.27, 8.5 before 8.5.12. watchTower and Cloudflare describe a wider range (PHP 5 onward); PHP's own advisories do not state it. PHP 8.1 and older get no PHP-project updates.

BRANCH	FIXED IN
PHP 8.2	8.2.35
PHP 8.3	8.3.36
PHP 8.4	8.4.27
PHP 8.5	8.5.12

Upstream PHP, then restart every PHP worker:

UBUNTU RELEASE / PACKAGE	FIXED IN
26.10 php8.5	8.5.9-0ubuntu2.1 USN-8948-1
26.04 LTS php8.5	8.5.4-0ubuntu1.5 USN-8948-1
24.04 LTS php8.3	8.3.6-0ubuntu0.24.04.13 USN-8948-1
22.04 LTS php8.1	8.1.2-1ubuntu2.28 USN-8948-1
20.04 php7.4	7.4.3-4ubuntu2.29+esm5 USN-8948-2 (Pro/ESM)

EDITION

Release baseline	2026-10-13
EPSS cutoff	2026-10-21
Edition	1

KEY FACTS

CVEs Microsoft published 13 Oct	1,415
Microsoft Critical	80
Exploitation Detected	1
KEV additions Oct 1-21	24
...by 13 Oct	11
...14 to 21 Oct	13
Findings	10
P1 / P2	9 / 1

SIGNAL LEGEND

P1 First response
Priority: editorial response window

Firewalls / VPN
Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical
CVSS: technical severity band

VENDOR Important
Vendor rating
1.512%  **74.24** pctl

EPSS: probability; bar = percentile rank
KEY exploited
KEV: catalog evidence of exploitation

§2.7 PHP (WEB SERVERS) · CONTINUED

UBUNTU RELEASE / PACKAGE	FIXED IN
18.04 php7.2	7.2.24-0ubuntu0.18.04.17+esm14 USN-8948-2 (Pro/ESM)
16.04 php7.0	7.0.33-0ubuntu0.16.04.16+esm22 USN-8948-2 (Pro/ESM)
14.04 php5	5.5.9+dfsg-1ubuntu4.29+esm18 USN-8948-2 (Pro/ESM)

Other distributions and hosting providers: not confirmed in this brief.

TEMPORARY EXPOSURE REDUCTION	PHP: updating is "the only complete mitigation". Vendor partial measures (they reduce exposure; they are not a fix): for 109618, set <code>memory_limit=-1</code> so applications can't override it (e.g. <code>php_admin_value</code> in the FPM pool or Apache config). For 109619, set <code>session.upload_progress.enabled=0</code> in <code>php.ini</code> or the FPM pool/server config (not <code>ini_set()</code> or <code>.user.ini</code>), and on 8.5 also <code>fatal_error_backtraces=0</code> . Restart every worker after any change. Cloudflare says it deployed WAF mitigations for its customers; that is a third-party measure, not a fix.
VALIDATION	Confirm the version actually serving web requests, not just the command-line <code>php -v</code> : e.g. the PHP-FPM or <code>mod_php</code> package version (general check). On Ubuntu, compare the installed package version with the USN version above (general check). Confirm every worker or pool restarted. Given the third-party exploitation reports, review internet-facing PHP servers that were unpatched on or after 21 Oct; the update does not prove a server was never compromised.
REFERENCES	php.net security advisory · GHSA-w8hw-w9fx-j79w · GHSA-6wmf-4rv5-p3rp · Ubuntu USN-8948-1 · USN-8948-2 · evulnable CVE-2026-109618 · evulnable CVE-2026-109619

P1 First response

WHO HAS THIS Remote support

§2.8

BeyondTrust Remote Support: improper origin validation

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2026-102764	BEYONDTTRUST Critical	9.3 Critical CVSS 4.0	1.180% 67.40 pctl · scored 2026-10-21	KEY exploited added 10-16 · due 10-19
PRIORITY	P1 because it is in CISA KEV (added 2026-10-16). BeyondTrust's advisory does not say whether it was exploited. No ransomware campaign use reported (CISA: Unknown).			
EXPOSURE AND IMPACT	BeyondTrust: an internal messaging component did not validate where messages came from, which could let a remote attacker perform file operations on the appliance. BeyondTrust's CVSS vector shows network access, no privileges and no user interaction (AV:N/PR:N/UI:N). This is remote-support infrastructure, i.e. a management service.			
PERMANENT REMEDIATION	BeyondTrust names a patch, not a version number: BT26-05-RS patch for v24.31-v26.2.3 (affected: all versions up to 26.2.3). Older than 24.3.1: upgrade first, then patch. SaaS was patched on 9 Oct 2026. Self-hosted servers without automatic updates must apply it manually from the / appliance interface.			
TEMPORARY EXPOSURE REDUCTION	No vendor workaround published; patch is the fix.			
VALIDATION	Confirm in the /appliance interface that the BT26-05-RS patch is installed (general check; BeyondTrust gives no verification step). CISA marks this CVE for forensic triage; review appliance logs separately, because the patch alone doesn't prove the appliance was never accessed.			
REFERENCES	BeyondTrust BT26-05 · evulnable CVE-2026-102764			

EDITION

Release baseline 2026-10-13
EPSS cutoff 2026-10-21
Edition 1

KEY FACTS

CVEs Microsoft published 13 Oct 1,415
Microsoft Critical 89
Exploitation Detected 1
KEV additions Oct 1-21 24
...by 13 Oct 11
...14 to 21 Oct 13
Findings 10
P1 / P2 9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pctl

EPSS: probability; bar = percentile rank

KEV exploited

KEV: catalog evidence of exploitation

P1 First response

WHO HAS THIS Backup servers

§2.9

AhsayCBS backup server: authentication bypass + command injection

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2026-105134	AHSAY not stated	10.0 Critical CVSS 4.0	4.782% 91.88 pctl · scored 2026-10-21	KEV exploited added 10-14 · due 10-17
CVE-2026-105133	AHSAY not stated	6.9 Medium CVSS 4.0	0.854% 57.86 pctl · scored 2026-10-21	KEV exploited added 10-14 · due 10-17

PRIORITY

P1 because both are in CISA KEV (added 2026-10-14) and CISA says they can be chained. CVSS scores are from the CNA (VulDB); Ahsay publishes none. No ransomware campaign use reported (CISA: Unknown, which does not mean none).

EXPOSURE AND IMPACT

CISA: a remote attacker can bypass authentication through the API's checkSysPwd function (105133), and can run operating-system commands through the Replication Receiver endpoint / rps/api/json/UpdateReceivers.do (105134). No user interaction is described. Reachability: the server's API / Replication Receiver service (Ports not published). The impact is on the backup server that holds client data.

PERMANENT REMEDIATION

AhsayCBS v10: hotfix v10.3.4.45. v7, v8 and v9: hotfix v9.15.2.70. Reboot after applying. Partner-portal login needed to download (Ahsay notice, 12 Oct 2026). Ahsay says its earlier patches v9.15.2.59 and v10.3.4.0 did not fully fix these.

TEMPORARY EXPOSURE REDUCTION

No vendor workaround published; patch is the fix. General measure (not a fix): allow only trusted networks to reach the AhsayCBS web and replication services.

VALIDATION

Confirm the management console shows AhsayCBS 10.3.4.45 or 9.15.2.70 and that the server has rebooted (general check; Ahsay gives no verification step). CISA marks 105134 for forensic triage. A server that was reachable before patching needs a separate compromise review; the hotfix does not prove it was never accessed.

REFERENCES

[Ahsay notice](#) · [evulnable CVE-2026-105134](#) · [evulnable CVE-2026-105133](#)

P2 Accelerated (7 days)

P2 Accelerated

WHO HAS THIS Office / Microsoft 365 Apps

§2.10

Microsoft Outlook: remote code execution via the Reading Pane

CVE	VENDOR RATING	CVSS	EPSS · OCT 21	KEV / EXPLOITATION
CVE-2026-97749	MICROSOFT Critical	9.8 Critical CVSS 3.1	0.977% 61.74 pctl · scored 2026-10-21	Not in KEV

PRIORITY

P2 because Outlook processes untrusted mail and this is a no-click remote code execution path. Microsoft: not exploited, not publicly disclosed, "Exploitation Less Likely". Not in CISA KEV (catalog 2026.10.21).

EXPOSURE AND IMPACT

Double-free remote code execution flaw in Outlook. Microsoft: an attacker sends a crafted email, and "simply viewing the message in the Outlook Reading Pane could trigger the vulnerability". No privileges needed and no click needed (UI:N).

§2.10 MICROSOFT OUTLOOK • CONTINUED

EDITION

Release baseline	2026-10-13
EPSS cutoff	2026-10-21
Edition	1

KEY FACTS

CVEs Microsoft published 13 Oct	1,415
Microsoft Critical	80
Exploitation Detected	1
KEV additions Oct 1-21	24
...by 13 Oct	11
...14 to 21 Oct	13
Findings	10
P1 / P2	9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pctl

EPSS: probability; bar = percentile rank

KEY exploited

KEV: catalog evidence of exploitation

PERMANENT REMEDIATION	PRODUCT / CHANNEL	FIXED IN
	Office LTSC 2024	16.0.17932.21056 MSRC
	Office LTSC 2021	16.0.14334.20974 MSRC
	M365 Apps Current Channel	Version 2609 (Build 20430.20182) 13 Oct 2026 release notes
	M365 Apps Monthly Enterprise	2609 (20430.20180) or 2608 (20326.20232) / 2607 (20228.20276); release notes

Microsoft 365 Apps: MSRC gives no build number; the 13 Oct 2026 release notes list this CVE.

TEMPORARY EXPOSURE REDUCTION	No vendor workaround published; patch is the fix. (Microsoft lists no workaround or mitigation.)
VALIDATION	In Outlook, File > Office Account > About shows the version and build; confirm it is at or above the fixed build for its channel (general check).

REFERENCES	MSRC CVE-2026-97749 · M365 Apps security release notes · evulnable CVE-2026-97749
------------	---

P3 Standard high and P4 Remaining cycle

No findings in this brief are placed in P3 or P4. Apply the rest of the October updates on your normal cycle.

Also added to CISA KEV in October (lower fit for most client networks; fixed versions not checked):

- Citrix NetScaler CVE-2026-88779 (denial of service; added 4 Oct).
- Atlassian Data Center products CVE-2026-21589 (added 15 Oct; EPSS 12.711%, 96.26 percentile, scored 2026-10-21).
- Plex Media Server CVE-2026-96652/96654/96655/96656 (added 20 Oct).
- Zammad CVE-2026-102489/102490 (added 2 Oct).
- EG Secure Solutions SiteGuard CVE-2026-106931 and Siemens Software Center CVE-2026-110936 (added 20 Oct).
- Older bugs added 8 Oct: ProFTPD CVE-2015-3306, ISC BIND CVE-2015-5477, Apache Struts CVE-2016-3081, ONLYOFFICE CVE-2021-3199 and Strapi CVE-2023-22894. An old CVE newly added to KEV does not necessarily mean a new patch.

What to do (checklist)

- ☐ P1: check every client for items §2.1–§2.9 (Windows, email gateways, firewalls/VPN, PHP websites/web apps, remote support, backup servers) and apply the fixes. For exposed appliances, also run the vendor's compromise checks.
- ☐ Confirm Windows PCs and servers show the fixed build and have restarted (§2.1).
- ☐ P2, within 7 days: update Office / Microsoft 365 Apps to the 13 Oct 2026 builds (§2.10).
- ☐ List clients on Windows 11 Home/Pro 24H2 and plan the move to 25H2 or later. Microsoft: KB5127648 is the last update for those editions.
- ☐ Send the client note above, edited to say what you actually did.

EDITION

Release baseline	2026-10-13
EPSS cutoff	2026-10-21
Edition	1

KEY FACTS

CVEs Microsoft published 13 Oct	1,415
Microsoft Critical	89
Exploitation Detected	1
KEV additions Oct 1-21	24
...by 13 Oct	11
...14 to 21 Oct	13
Findings	10
P1 / P2	9 / 1

SIGNAL LEGEND

P1 First response

Priority: editorial response window

Firewalls / VPN

Who has this: how common the product is among MSP-managed clients (editorial)

CVSS 3.1 9.8 Critical

CVSS: technical severity band

VENDOR Important

Vendor rating

1.512% 74.24 pctl

EPSS: probability; bar = percentile rank

KEV exploited

KEV: catalog evidence of exploitation

Claim-to-source note. Every score, date, version and quote above traces to a row in the source list (available on request), with its URL and UTC fetch time. Every cover figure traces to the source list (rows 1, 5, 6, 23, 25 and 37).

CLAIM TYPE	SOURCE LIST ROWS
Vendor advisories	10-16
PHP finding (§2.7)	27-35
Microsoft fix data	1-4 and 17-19
CISA KEV	5
FIRST EPSS	6, 7 and 22
CVE records	23
KB5127648	24
Release counts	25 and 37
EPSS definition	26

Sources:

- PHP: php.net advisory, php-src GitHub advisories, CVE records, Ubuntu USN-8948-1/-2, watchTowr, Cloudflare.
- Vendor advisories: Ahsay; Fortinet FG-IR-26-175 and FG-IR-26-122; Cisco cisco-sa-esa-afw-zqYJkxjp; BeyondTrust BT26-05; Ivanti; Palo Alto CVE-2026-0322.
- Microsoft: MSRC October 2026 data (rev. 21 Oct 2026), KB5127648 and the Microsoft 365 Apps security release notes.
- CISA KEV catalog v2026.10.21; FIRST EPSS (scored 2026-10-21); CVE Program records; Microsoft Lifecycle.

Data cutoff: 21-22 Oct 2026 UTC.

This brief is informational only. It reports what public sources say. It does not check your systems, does not make anyone compliant with any standard, and does not guarantee anyone is or will stay secure. Patches were not tested in any client environment. Confirm details in each vendor's advisory before acting. Reviewed by a person before release.