Black Cat

Week 33, 2026
7–14 August

This week at a glance

Black Cat threat data | 7–14 August 2026

10	Claimed ransomware attacks affecting SMBs this week
4	New actively exploited vulnerabilities
0	Vulnerabilities marked ransomware linked this week

Executive Summary

Microsoft's monthly Patch Tuesday update is a useful prompt to review routine patching, but this week some systems need faster action. The immediate priority is active exploitation of on-premises Microsoft SharePoint Server. Apply the relevant fix, determine whether the server was exposed to the internet, rotate credentials for exposed systems and carry out a compromise review.

Threat level
High

The wider priority is systems that either face the internet or manage many devices: Cisco ASA/FTD firewalls, Windows endpoints, Ivanti management platforms and VMware vCenter. CISA has also recorded active exploitation of a Cisco firewall issue and a Windows privilege-escalation flaw. ShieldBreak is not an entry route on its own, but it could make an existing compromise more damaging while Microsoft assesses the claim.

Black Cat recorded 10 claimed ransomware-victim listings affecting organisations in SMB employee-size bands during this reporting window. CISA added four KEV entries; none has yet been marked as used in a ransomware campaign.

CISA exploited-vulnerability watch

Four new KEV entries this week — two need immediate attention in this report.

CVE-2026-8037 · Cisco ASA/FTD CVE-2026-20349 · Windows CVE-2026-68820 · CVE-2026-72898

4	**New KEV entries**	Added during Week 33
2	**Report priorities**	Cisco ASA/FTD and Windows
0	**New ransomware flags**	All four remain Unknown

Top Story

Patch Tuesday: prioritise exposed and management systems first

What happened: Patch Tuesday is Microsoft's regular monthly release of security updates. This month, do not treat every update alike. Active exploitation of CVE-2026-50522 affects on-premises SharePoint Server, while other urgent checks concern Cisco ASA/FTD firewalls and Windows devices. Ivanti and VMware customers should also confirm the vendor fixes that apply to their management systems.

Why it matters: An externally exposed collaboration server, firewall or management platform can give attackers a route to business data, remote access or many managed endpoints. Microsoft 365 SharePoint Online is not the on-premises SharePoint Server product named in the advisory.

What to do: Ask your IT provider for written confirmation of whether the business uses on-premises SharePoint Server, Cisco ASA/FTD, Ivanti Neurons for MDM or Endpoint Manager, or VMware vCenter. For each relevant product, ask for the fixed version or mitigation, whether it was internet-exposed, and whether a compromise review is needed. SharePoint should be treated as an incident-response check as well as a patching task.

Patch Tuesday: triage by business impact

Prioritise systems that are exposed to the internet or manage many devices.

1	**Treat as an incident**	**SharePoint Server** Patch, check exposure and review compromise.
2	**Expedite fixes**	**Cisco firewall and Windows** Protect edge services and endpoints.
3	**Plan and verify**	**Ivanti and VMware** Name an owner and confirm completion.

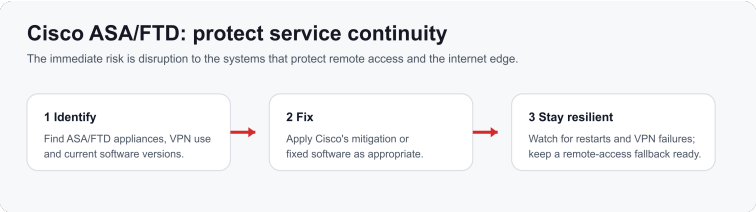
Top Threats This Week

1. Cisco firewall issue: confirm ASA/FTD status and service resilience

What it means: CISA has added CVE-2026-20349 affecting Cisco ASA and Secure Firewall Threat Defense (FTD) to its KEV catalog. The reported effect is a remotely triggered denial-of-service condition. An attacked firewall can interrupt remote working, customer connectivity and security monitoring at exactly the time the business needs them.

Who should pay attention: Any organisation or IT provider using Cisco ASA or FTD, especially where the appliance provides VPN or internet-edge security services. GreyNoise and RansomGrok context shows continued hostile attention on older Cisco and Fortinet edge-device vulnerabilities. That is not evidence that this new Cisco flaw is being scanned.

Action: Confirm whether the affected Cisco software is deployed, apply Cisco's mitigation or fixed software, and check monitoring for unexplained appliance restarts, failed VPN connections or availability alerts. Keep an agreed fallback for remote access and firewall management.

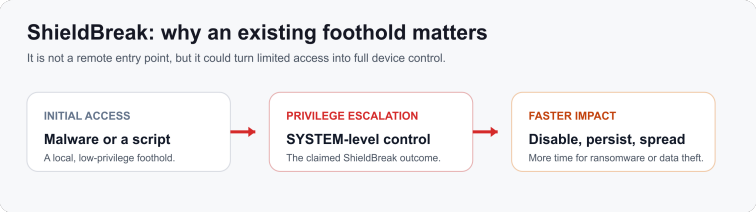


2. ShieldBreak: a Microsoft Defender patch-bypass that could accelerate a compromise

What it means: A researcher publicly released a proof of concept called ShieldBreak shortly after Patch Tuesday. It is reported to bypass the earlier Microsoft Defender RoguePlanet fix and give a low-privileged local user SYSTEM-level control. This is not a way to break into a business remotely: an attacker first needs initial access through another mechanism. If valid, the bypass could make subsequent attacks, including ransomware, quicker and easier.

Who should pay attention: Every organisation using Windows, particularly those that rely on Microsoft Defender and an IT provider for endpoint monitoring. An attacker who already has a limited presence could tamper with security controls, create persistence and gain wider access much faster.

Action: Keep a close eye for an out-of-band patch and apply it promptly. Ask your IT provider to confirm its ShieldBreak detection and mitigation position, and investigate unexpected SYSTEM-level processes, Defender configuration changes, untrusted scripts and attempts to disable endpoint protection. Do not disable Defender as a workaround.

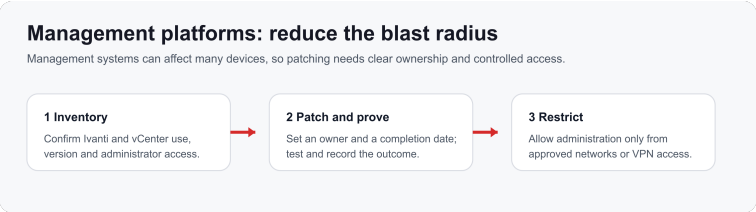


3. Management platforms: patch Ivanti and VMware where they are in use

What it means: Ivanti has issued August fixes for Neurons for MDM and Endpoint Manager (EPM), while Broadcom has supplied fixes for VMware vCenter CVE-2026-59310. Ivanti reports no evidence of exploitation for its update at this time. vCenter is a high-value management platform because it can affect many systems at once.

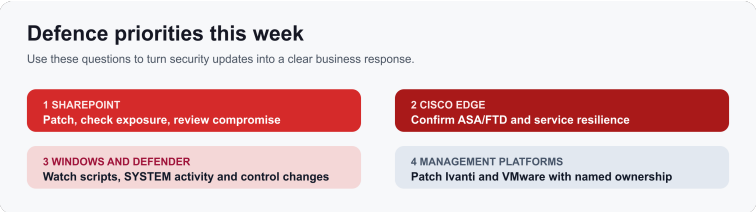
Who should pay attention: Organisations using Ivanti, virtual servers or central endpoint management. These systems can hold powerful credentials and affect many business devices, creating a wide operational risk.

Action: Confirm product use and installed versions, test and apply the relevant vendor update promptly, and restrict management interfaces to approved administrator networks or VPN access. Record who is responsible for applying the update and confirming completion.



Recommended Actions

- Treat on-premises SharePoint as urgent if exposed externally. Apply the relevant update, identify past internet exposure, rotate credentials for exposed instances and complete a compromise review.
- Check the internet edge. Confirm whether Cisco ASA/FTD is deployed, apply the vendor mitigation or fixed software, and ensure a firewall outage has a documented response plan.
- Maintain endpoint defences. Apply Windows and Defender updates promptly; monitor for suspicious scripts, SYSTEM-level processes and changes to security controls while ShieldBreak's remediation status is clarified.
- Patch management platforms on a named timetable. Confirm the Ivanti and VMware versions in use, restrict their management interfaces and document the approved update owner and completion date.



Plain English Notes

Patch Tuesday: Microsoft's regular monthly release of security updates. It is a scheduling point, not a guarantee that every vulnerability can safely wait for normal testing.

Known Exploited Vulnerability (KEV): A vulnerability that CISA has evidence is being used in real attacks. It should be prioritised above an ordinary software flaw.

SYSTEM-level control: The highest level of control on a Windows computer. Attackers who reach it can often interfere with security tools and access data that a normal user cannot.

Further Reading

The primary sources supporting this briefing are listed below.

Vulnerabilities mentioned in this report

Vendor	Product	CVE	KEV status	Ransomware use
Microsoft	SharePoint Server	CVE-2026-50522	Previously added	Unknown
Cisco	ASA / FTD	CVE-2026-20349	New W33	Unknown
Microsoft	Windows	CVE-2026-68820	New W33	Unknown
Progress	LoadMaster	CVE-2026-8037	New W33	Unknown
Metabase	Metabase	CVE-2026-72898	New W33	Unknown
VMware	vCenter	CVE-2026-59310	Not KEV	Not stated
Microsoft	Defender engine	CVE-2026-50656	Not KEV	Not stated

Sources

- Microsoft: SharePoint Server Subscription Edition security update and CERT-EU: critical Microsoft SharePoint vulnerabilities.
- CISA Known Exploited Vulnerabilities catalog — Cisco ASA/FTD CVE-2026-20349 and Microsoft Windows CVE-2026-68820.
- Ivanti August 2026 security update and Broadcom vCenter remediation.
- Arctic Wolf: RoguePlanet and ShieldBreak and NVD: CVE-2026-50656.