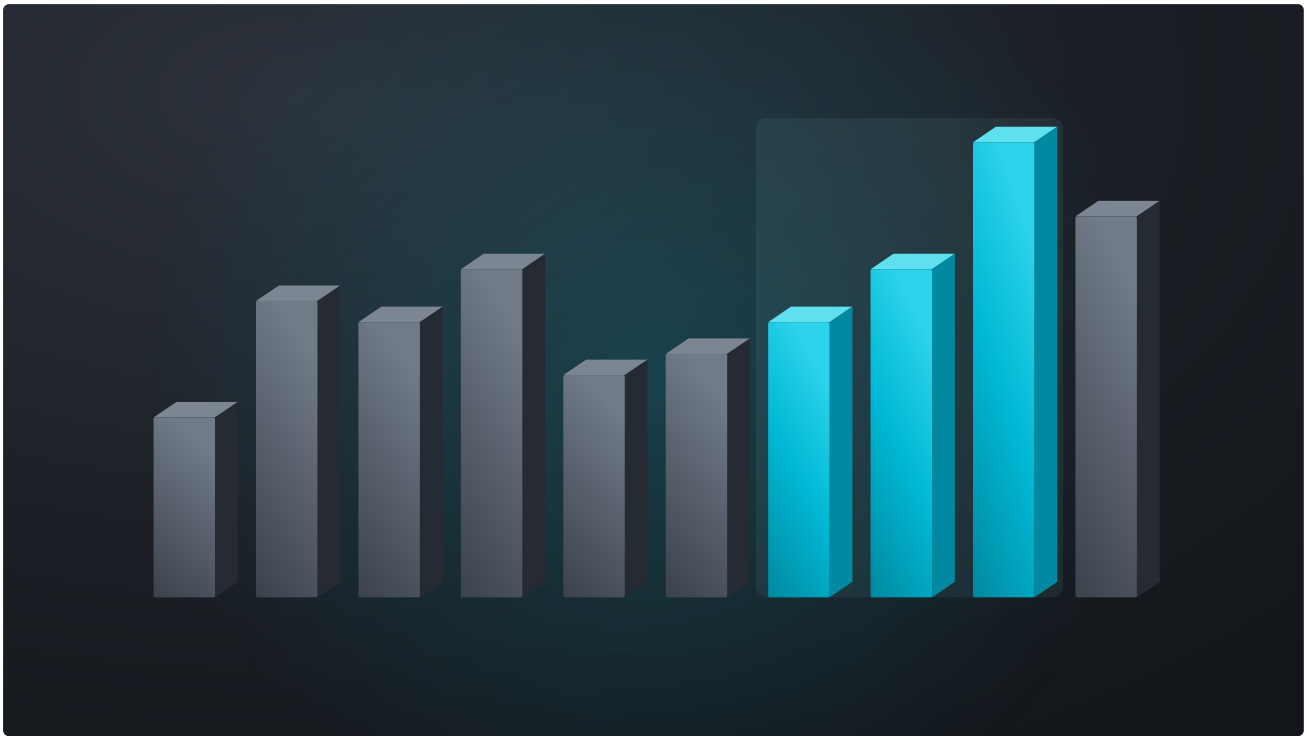
Black Shard

RESEARCH REPORT

Known exploited vulnerabilities, July to September 2026: what the CISA catalogue says about the office boundary

The list of vulnerabilities confirmed as exploited grew faster from July to September 2026 than in either earlier quarter of the year, and a quarter of the additions came from the makers of the firewalls, gateways and routers that stand between a small firm and the internet.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-14
Classification	Public
Version	1.1
First published	11 November 2026
This edition	16 November 2026
Figures	Additions dated 1 Jul to 30 Sep 2026, read 11 Nov 2026

Executive summary

CISA added 100 vulnerabilities to its Known Exploited Vulnerabilities catalogue between 1 July and 30 September 2026, across 48 vendors. The additions ran 26 in July, 31 in August and 43 in September.

The catalogue took 71 additions from January to March 2026, 75 from April to June and 100 from July to September, the most of the three quarters. The 100 additions are 41 per cent more than the 71 of January to March 2026, and 96 per cent more than the 51 the catalogue took between 1 July and 30 September 2025.

Six vendors whose products include the firewalls, routers and remote access gateways on the office boundary, Cisco, Citrix, Fortinet, SonicWall, MikroTik and Check Point, account for 25 of the 100 additions. Those are the devices an attacker reaches from the internet without anyone at the firm opening an email or clicking a link. A firewall, a VPN gateway and a remote access appliance answer anyone who connects, by design, and a flaw in one is scanned for across the internet within days of a working exploit becoming public.

From Maturity Level 1, the Essential Eight requires patches for vulnerabilities in online services within 48 hours of release when the vendor rates the flaw critical or a working exploit exists, and within two weeks otherwise. An entry in the catalogue is a working exploit by definition, so every addition that touches a device on the boundary starts the two-day clock on the day the vendor’s fix is released.

A small firm keeps that clock with three things in place before the entry lands: a list of what sits on its boundary, with the vendor and the firmware version of each device; a person allowed to patch a firewall or gateway outside the monthly cycle; and a plan for the device whose fix cannot land in two days.

- List every device and service that faces the internet: the firewall, the VPN or remote access gateway, the router, any server published to the internet, and the management consoles that run them.
- Match the catalogue feed against that list every week, and give each match on the boundary a due date two days out.
- Keep the management interface of every boundary device off the internet, so a flaw in the console needs an attacker already inside.

Method

The Known Exploited Vulnerabilities catalogue is kept by the Cybersecurity and Infrastructure Security Agency in the United States. An entry needs three things: a CVE identifier, reliable evidence that attackers have used the flaw against real systems, and a fix or mitigation from the vendor. The catalogue carries no severity score, because every entry has already been used. Australian guidance treats the same evidence the same way: a flaw with a working exploit in an internet-facing service goes into the shortest patch window the Essential Eight sets.

We read the catalogue’s public JSON feed on 11 November 2026, in the version CISA released on 9 November 2026, and took every entry whose date added falls between 1 July and 30 September 2026. The entries were counted by calendar month and by the vendor name the catalogue gives each one; a vendor with several affected products counts once in the vendor count. The date added never changes once an entry is listed, so the counts for the quarter are the same in every later version of the catalogue. The two earlier quarters of 2026, the months to October and the same quarter of 2025 were counted from the same version, the same way.

The ransomware figure is the catalogue’s own flag for entries CISA has tied to a known ransomware campaign, as it stands in the version we read. CISA sets the flag when the evidence arrives, which can be months after the entry is

listed, so the count for a recent quarter starts low and rises. The date added is the day CISA listed the entry; the flaw may have been exploited for weeks before that. Every figure here is a floor, and no CVE is named, because the point is the volume and where it falls.

Run the same match against your own boundary

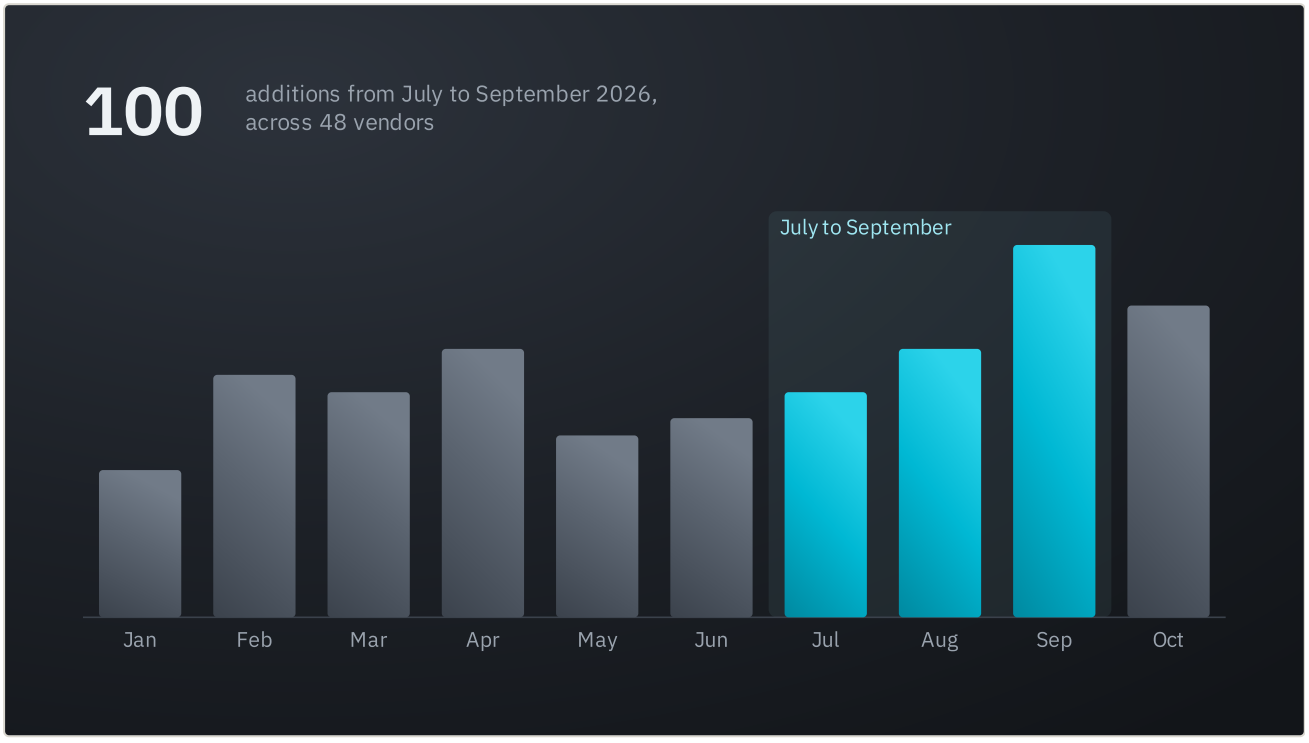
The feed is a file anyone can download, and it carries the vendor, the product and the date added for every entry. Write down every device and service your firm exposes to the internet, with its vendor, model and firmware version, including the ones a provider runs for you: the office firewall, the VPN or remote access gateway, the router at each site, the email gateway, any server published for staff or clients, and the consoles that manage them. Match the feed's vendor and product fields to that list each week and open a ticket for every match.

A match on a boundary device is due in two days at every maturity level. A match elsewhere takes the window the maturity model sets for that class of software. Where the vendor has published a fix and it cannot be applied in time, the compensating step is the same each time: restrict the device to known addresses, turn off the affected feature, or take the service off the internet until the fix is in.

The list is where the match usually breaks. A patch report from the desktop management tool covers the laptops and says nothing about the firewall, whose firmware is updated by whoever installed it, when they remember. The boundary devices in the catalogue are the ones nobody owns on paper.

The quarter, month by month

ADDITIONS BY MONTH, JANUARY TO OCTOBER 2026



September set the high for the year to October; the quarter took 100 additions, up from 71 in January to March. Source: CISA Known Exploited Vulnerabilities catalogue, additions dated 1 July to 30 September 2026, read 11 November 2026.

The additions ran 26 in July, 31 in August and 43 in September. September's 43 additions are the most of any month from January to October 2026.

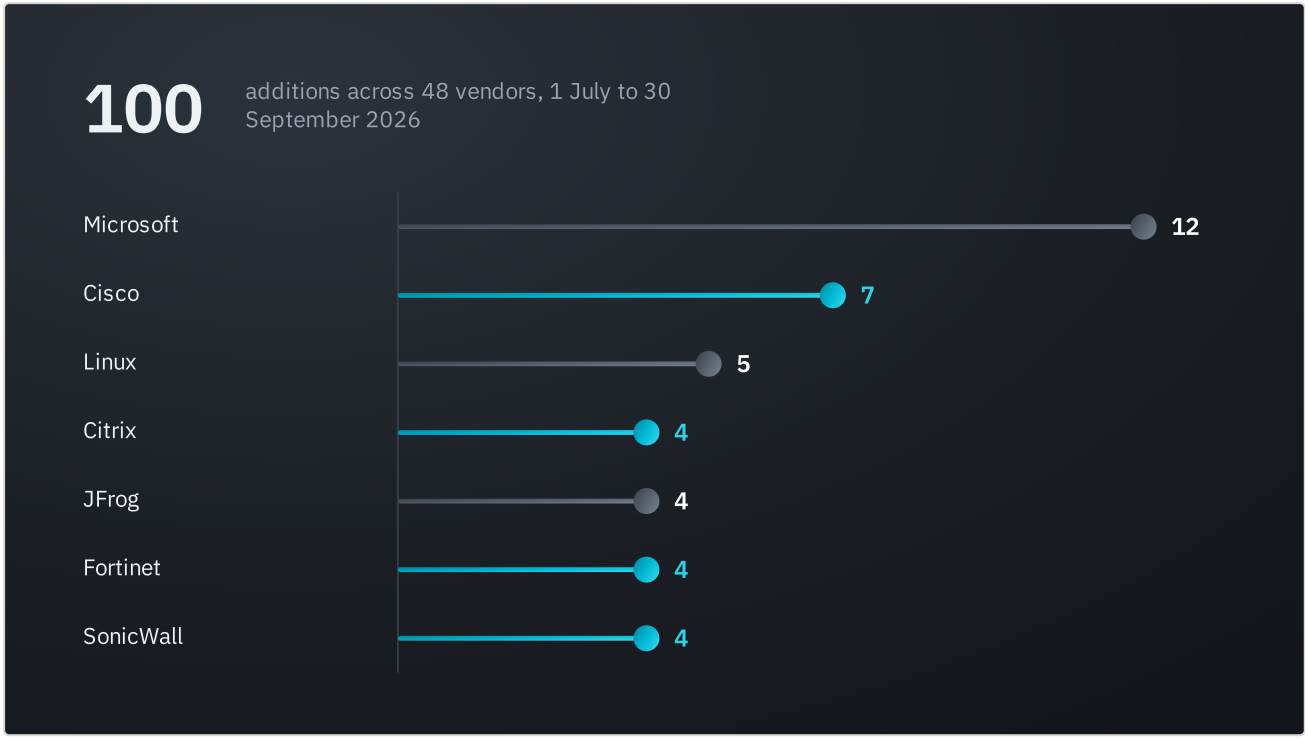
Month by month from January to October 2026 the catalogue took 17, 28, 26, 31, 21, 23, 26, 31, 43 and 36 additions, 282 in the ten months. The quarter averaged 33 additions a month, three for every two working days. A firm that patches its boundary devices once a quarter, or when a contractor next visits, works through a list that grows by that much between visits, and the two-day entries on it have been open the whole time.

July's 26 additions came from 16 vendors, August's 31 from 23 and September's 43 from 25. The quarter widened as it went. Each month drew its additions from more vendors than the one before, and a wider spread means more of the long tail: products a small firm installed once and stopped thinking about.

In the catalogue version of 9 November 2026, six of the 100 additions carry the flag for use in known ransomware campaigns: four of July's, two of August's and none of September's. The flag is a late signal. Ransomware crews use whatever is in the catalogue once an exploit is public, and the evidence that ties a flaw to a named campaign usually arrives after the damage, so a quarter with few flagged entries is a quarter whose evidence is still coming in.

Where the additions sit

ADDITIONS BY VENDOR, JULY TO SEPTEMBER 2026



Microsoft heads the quarter; the seven vendors with four or more additions account for 40 of the 100, and the four in cyan make boundary devices. Source: CISA Known Exploited Vulnerabilities catalogue, additions dated 1 July to 30 September 2026, read 11 November 2026.

Microsoft accounted for 12 of the 100 additions, Cisco for 7 and the Linux kernel for 5; Citrix, JFrog, Fortinet and SonicWall had 4 each. The seven vendors with four or more additions account for 40 of the 100; the other 41 vendors share the remaining 60, and 28 of them have a single entry.

Six of Microsoft's 12 additions in the quarter were in SharePoint; the other six were spread across Windows, SQL Server and Active Directory Federation Services. SharePoint in the cloud is patched by Microsoft. A SharePoint server a firm runs in its own office or rack is patched by the firm, and the servers that still run that way are often the ones published to the internet so staff can reach documents from home. The same reading applies to an Active

Directory Federation Services server: it exists to answer sign-ins from outside, so it sits on the boundary whether the firm thinks of it that way or not.

The Linux kernel's entries reach a small firm through the devices built on it: the network storage box in the comms cupboard, the router, the firewall and the appliances a vendor ships as a closed box. JFrog Artifactory, a store for the software a development team builds, appears for the firms that write their own code. N-able N-central, the console many IT providers use to manage their clients' computers, appears as well, and a flaw in a provider's console is a flaw in every client it manages.

The boundary, vendor by vendor

Six vendors whose products include the firewalls, routers and remote access gateways on the office boundary, Cisco, Citrix, Fortinet, SonicWall, MikroTik and Check Point, account for 25 of the 100 additions.

Read by product, the six vendors' entries are the equipment of an ordinary office network. Cisco's are firewalls, the consoles that manage them, an SD-WAN manager, its network access control server, the router operating system and an email gateway. Citrix's are NetScaler, the gateway many firms use to publish remote desktops. Fortinet's include FortiOS, the operating system of its firewalls. SonicWall's are its SMA remote access appliances. MikroTik's are RouterOS, which runs on routers sold widely to small offices. Check Point's include its firewall management console.

> A boundary device answers anyone on the internet. When its flaw is in the catalogue, the fix, or the step that takes the device off the internet until the fix is in, is due in two days.

Several of the quarter's boundary entries are in management consoles, the software used to configure the firewalls. A console reachable from the internet gives an attacker who exploits it the rules of every device it manages. A console reachable only from inside the network, or only through a separate administrative connection, needs an attacker who is already in. Moving the console off the internet is a one-off change that moves it out of the two-day class.

The firmware cycle is the other half. Many small firms update a firewall only when it is replaced or when the installer next visits. A gateway in the catalogue needs its update within two days, which means the person who can apply it is named in advance, the vendor's support entitlement that unlocks the firmware download is current, and a rollback is known if the update fails. An appliance past the end of the vendor's support receives no fix at all; its only answer is replacement.

What to do

1. Write down every device and service that faces the internet, with its vendor, model and firmware version: the firewall, the VPN or remote access gateway, the router at each site, the email gateway, any server published to the internet, and the consoles that manage them.
2. Subscribe to the catalogue feed and match it against that list every week. A match on the boundary opens a ticket due in two days; any other match takes the window the maturity model sets for its class of software.
3. Name the person who may update a boundary device outside the cycle and the person who approves it, and confirm the vendor support that unlocks each device's firmware is current.

4. Move every management console off the internet: reachable from the internal network or a separate administrative connection only.
5. Write the compensating step for each boundary device when a fix cannot land in two days: restrict it to known addresses, turn off the affected feature, or take the service off the internet.
6. Replace every boundary device the vendor no longer supports. It will not receive a fix for the next entry.
7. Ask your IT provider in writing how it patches the console it uses to manage your computers, and how it tells you when that console is in the catalogue.

We run patching to the Essential Eight windows for clients, with the catalogue matched against their inventory each week and every match worked to its due date, and our attack surface monitoring watches what a client exposes to the internet so the match is made against what an attacker can reach. An Essential Eight assessment reads the patch windows back from the live systems and sets the uplift in order. Scope and price are at blackshard.com.au/essential-eight-assessment.

Our record

Black Shard builds and defends the systems Australian organisations run on.

The record is as held at 16 November 2026, the date this edition was revised.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027.
- Essential Eight Maturity Level 3, assessed September 2026.
- Prequalified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Approved supplier on the Tasmanian Government Technology Services List (TSL) for Application Development Services, Operational Technical Services and Cyber Security.
- Our CISO holds the Exemplar Global ISO/IEC 27001:2022 Lead Auditor credential.
- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.
- More than 1,500 deploys and releases shipped since 27 April 2026.

> 24/7 incident line: 1800 370 270.

Sources

- CISA, Known Exploited Vulnerabilities Catalog, JSON feed, catalogue version of 9 November 2026, additions dated 1 July to 30 September 2026, read 11 November 2026: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
- CISA, Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

— CISA, Binding Operational Directive on reducing the significant risk of known exploited vulnerabilities, 3 November 2021: https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities
— Australian Signals Directorate, Essential Eight maturity model (November 2023), 27 November 2023: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model