Black Shard

RESEARCH REPORT

Known exploited vulnerabilities, January to March 2026: what the CISA catalogue says about the patching clock

In the first three months of 2026 the list of vulnerabilities confirmed as exploited grew faster than one a working day, and the vendors at the top of it make the desktop, the phone and the firewall of an ordinary small firm. The Essential Eight sets its patch windows against this clock.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-08
Classification	Public
Version	1.2
First published	14 April 2026
This edition	16 November 2026
Figures	Additions dated 1 Jan to 31 Mar 2026

Executive summary

CISA added 71 vulnerabilities to its Known Exploited Vulnerabilities catalogue between 1 January and 31 March 2026, across 38 vendors. The additions ran 17 in January, 28 in February and 26 in March.

Microsoft accounted for 12 of the 71 additions, Apple for 7 and Cisco for 4; Synacor, Google, SolarWinds and SmarterTools had 3 each. The seven vendors with three or more additions account for 35 of the 71; the other 31 vendors share the remaining 36, most of them with a single entry.

The catalogue is a short list by design. An entry is a flaw that an attacker has already used against a real system, with a fix available, and nothing else qualifies. Read that way, the quarter is a count of the doors that opened in software a small firm runs: Windows and Microsoft 365 on the desks, iPhones in pockets, a Cisco or equivalent appliance on the office boundary, and a mail server or helpdesk tool somewhere that nobody has logged into for a year.

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 the definition of a working exploit, so each addition that touches an online service starts the two-day clock on the day it lands.

A small firm meets that clock by preparation. Every one of the quarter's additions was matched to a firm's own software, or missed, by whether the firm had an inventory to match it against, a person allowed to patch outside the monthly cycle, and a plan for the service that could not be patched in time.

- Keep an inventory of every product you run or rent, with its vendor and version, including the devices on the office boundary and the services a provider patches for you.
- Match the catalogue feed against that inventory every week and give each match a due date from the Essential Eight windows.
- Decide now who may patch out of cycle, how a change is reversed, and what happens to an exposed service when the fix cannot land in two days.

Method

The Cybersecurity and Infrastructure Security Agency in the United States keeps the Known Exploited Vulnerabilities catalogue under a binding directive it issued to federal agencies in November 2021. A vulnerability goes on the list when it has a CVE identifier, there is reliable evidence that it has been exploited against real systems, and the vendor has published a fix or a mitigation. The catalogue carries no severity score. Every entry is past the question of whether an attacker could use it.

The feed records the day CISA added each entry, and that date never changes, so the count of entries added between 1 January and 31 March 2026 is the same in every later version of the catalogue. We counted those entries, grouped by calendar month and by the vendor name the catalogue gives each entry. The vendor count is the number of distinct vendor names; a vendor with several affected products counts once. The ransomware figure is the catalogue's own flag for entries CISA links to a known ransomware campaign, as it stands in the catalogue version of 28 October 2026; CISA sets the flag when evidence arrives, so the count rises over time.

The date of addition is the day CISA listed the entry. The flaw itself may have been public, and exploited, for weeks or years before that, and the catalogue holds only what CISA has confirmed, so every figure here is a floor. No CVE is

named. The point is the volume and where it falls.

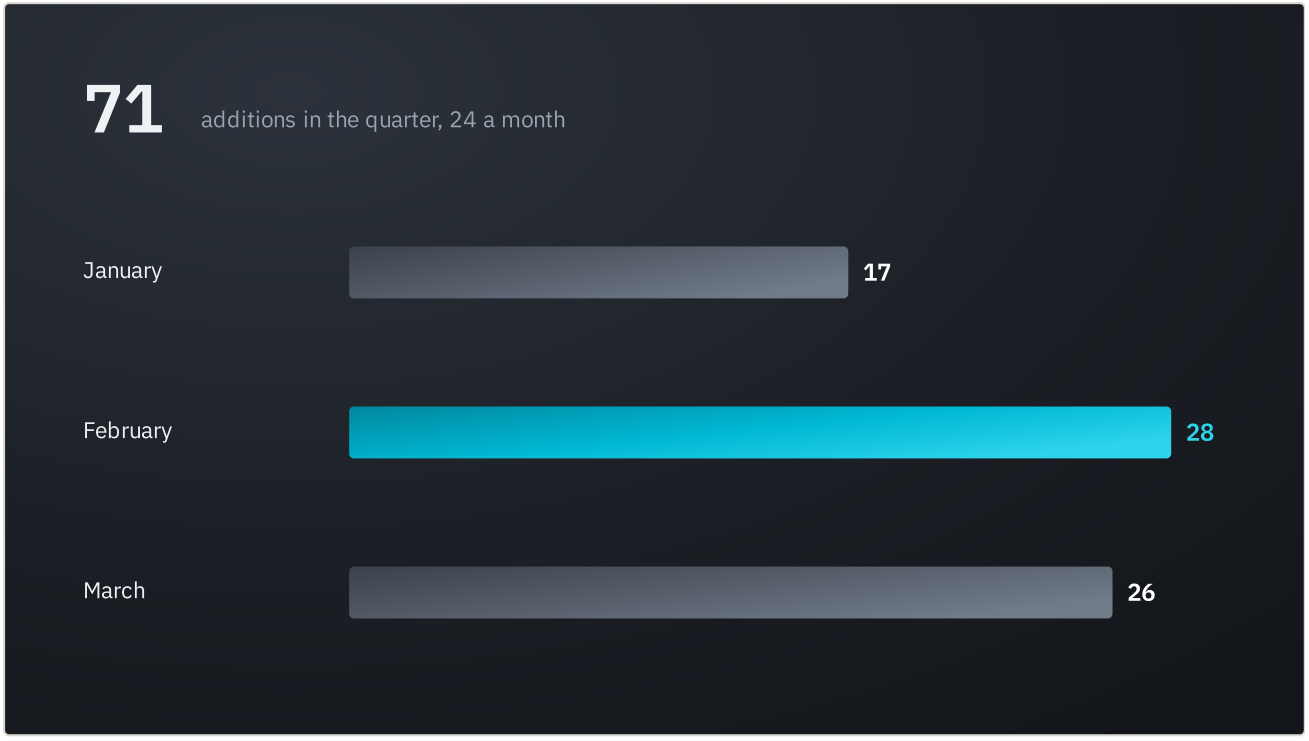
The same count is worth running in your own estate every week, against your own inventory. Download the feed, match the vendor and product fields to the software, devices and hosted services you hold, and open a ticket for every match. A match on an online service, an internet-facing server or a network device starts the two-day clock at every maturity level; a match on anything else takes the window the maturity model sets for that class of software, and at Level 3 the critical and exploited flaws in the common desktop applications move to two days as well. The feed carries CISA's own due date for US agencies; the Essential Eight clock is the one an Australian firm is assessed against.

The match is only as good as the inventory. A feed matched against a spreadsheet of laptops finds Microsoft and Apple and nothing else, because the firewall, the VPN gateway, the mail server and the tools a contractor installed were never written down. Those are the entries in the tail of the vendor table, and they are the ones that go unpatched.

The quarter, month by month

CISA added 71 vulnerabilities to its Known Exploited Vulnerabilities catalogue between 1 January and 31 March 2026, across 38 vendors. The additions ran 17 in January, 28 in February and 26 in March.

ADDITIONS BY MONTH, JANUARY TO MARCH 2026



February and March each added more than January; the quarter ran at 24 a month, against 20 a month in 2025. Source: CISA Known Exploited Vulnerabilities catalogue, additions dated 1 January to 31 March 2026.

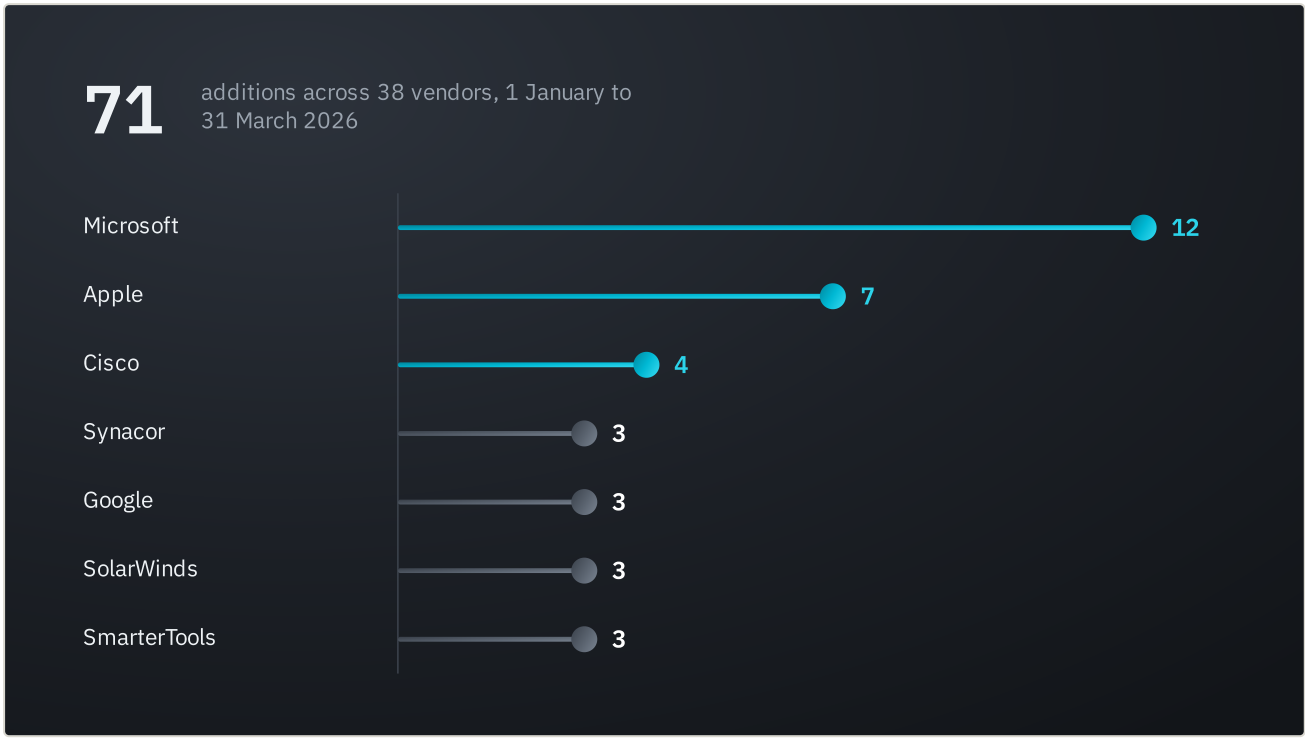
The quarter averaged 24 additions a month, more than one for each working day; across the whole of 2025 the catalogue took 245 additions, 20 a month. Twenty-four a month is the rate at which the list a firm must check against its own inventory grew, and every match on an online service or an internet-facing device is a two-day fix. A firm that patches on a monthly cycle meets that clock only by luck, when the vendor's fix happens to land just before its cycle runs.

In the catalogue version of 28 October 2026, six of the 71 additions carry the flag for use in known ransomware campaigns, two in each of the three months. Two a month is a small number and a misleading one. The flag marks entries CISA has tied to a named ransomware campaign, and CISA sets it when the evidence arrives, which can be months after the entry, so the figure is read from the current catalogue and rises over time. The operators who run ransomware against small firms use whatever is in the catalogue once a working exploit is public, and they rarely leave a name.

Where the additions sit

Microsoft accounted for 12 of the 71 additions, Apple for 7 and Cisco for 4; Synacor, Google, SolarWinds and SmarterTools had 3 each. Microsoft, Apple and Cisco together account for 23 of the 71 additions, 32 per cent of the quarter.

ADDITIONS BY VENDOR, JANUARY TO MARCH 2026



Microsoft, Apple and Cisco head the quarter; the seven vendors with three or more additions account for 35 of the 71. Source: CISA Known Exploited Vulnerabilities catalogue, additions dated 1 January to 31 March 2026.

The seven vendors with three or more additions account for 35 of the 71; the other 31 vendors share the remaining 36, most of them with a single entry. January's 17 additions came from 14 vendors, February's 28 from 16 and March's 26 from 20. The quarter widened as it went: each month drew its additions from more vendors than the month before, and the three months together touched nearly twice as many vendors as March alone.

Microsoft's place at the top is a function of how much Microsoft software exists, and the same is true of Apple and Cisco. For a small firm those three vendors are the whole stack: the desktops and the tenant, the phones, and the appliance on the office boundary. A firm cannot choose to be outside this list, because it runs the software.

The tail is the more instructive part. Synacor, SmarterTools and Roundcube make mail servers and webmail, software a small firm installed years ago on a box in the office or at a hosting provider, and SolarWinds makes the network monitoring and helpdesk tools IT contractors run for the firms they look after. These are the systems

nobody owns and nobody patches on a schedule, and an attacker who takes a mail server reads every invoice and every password reset that passes through it.

Cisco's entries, with Ivanti, Fortinet and Citrix further down the table, are the firewalls, VPN gateways and load balancers that face the internet by design. An attacker reaches them without any user opening anything, and a flaw in one is used at scale within days of the exploit becoming public. A quarterly firmware cycle on an internet-facing appliance is a standing loss against a two-day clock.

Why the windows are short

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.

The windows are set by how fast exploitation follows disclosure. The November 2023 edition of the maturity model shortened the window for applications that handle untrusted internet content from one month to two weeks, and added flaws the vendor rates critical to the two-day clock that already applied where a working exploit exists, at every maturity level. Those changes followed the same observation the catalogue makes every month: the gap between a vendor's advisory and mass exploitation of the flaw is now measured in days.

> Every catalogue entry is a working exploit by definition. For an online service, the two-day clock starts the day the vendor's fix is released.

Two days is achievable for a small firm, and only with decisions made before the entry lands. Who may apply a patch outside the cycle, and on whose say. What the rollback is when the patch breaks the service. Which systems are exposed to the internet, so the two-day cases are known before they arrive. What the compensating step is when the fix cannot land in time: restrict the service to known addresses at the boundary, disable the vulnerable component, or take it offline until the patch has settled elsewhere.

The two-week window is the ordinary case and the one most firms miss by habit. A monthly patch cycle is two weeks late half the time. Moving the cycle to fortnightly, with the two-day path alongside it for the catalogue matches, is the change that brings a small firm inside the model's first level.

What to do

1. Write down every product you run or rent, with its vendor and version: the desktops and their applications, the phones, the firewall and VPN gateway, the mail and file servers, the tools a contractor installed, and the hosted services whose patching belongs to someone else.
2. Subscribe to the catalogue feed and match it against that inventory every week. A match on an internet-facing system opens a ticket due in two days; any other match takes the window the maturity model sets for that class of software.
3. Name the person who may patch outside the cycle and the person who approves it, and rehearse one out-of-cycle patch so the path is known before a Friday afternoon entry lands.
4. Write the rollback for each exposed service and the compensating step when a fix cannot land in time: restrict it at the boundary, disable the component, or take it offline.
5. Ask each hosted provider in writing how it handles a catalogue entry for the software it runs for you, and how it tells you.

6. Retire what the vendor no longer supports. An unsupported product on the catalogue has no patch coming, and the maturity model removes it at every level.
7. Read the windows back from the systems: the date of the last applied patch on each device and service against the vendor's release date, every month.

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, additions dated 1 January to 31 March 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