NCSC and allies reveal most common cyber vulnerabilities exploited in 2022

New advisory highlights how threat actors exploited a larger number of older software vulnerabilities rather than more recently disclosed flaws last year.

- New joint advisory lists the top 12 vulnerabilities that were routinely exploited in 2022
- GCHQ's National Cyber Security Centre and partners reveal trend in attackers targeting older vulnerabilities rather than recently disclosed flaws
- UK organisations are encouraged to follow mitigation advice and sign up for the Early Warning service to bolster resilience

The UK and allies have issued a fresh warning to organisations today (Thursday) about the importance of updating systems after malicious cyber attackers were seen routinely targeting older software vulnerabilities in 2022.

In a new joint advisory, the National Cyber Security Centre – a part of GCHQ – and agencies in the US, Australia, Canada and New Zealand have revealed a list of the top 12 vulnerabilities that were routinely exploited last year.

More than half of the top vulnerabilities listed for 2022 also appeared on the previous year's list, highlighting how malicious cyber actors continued targeting previously disclosed flaws in internet-facing systems – despite security updates being available to fix them.

Attackers generally see the most success exploiting known vulnerabilities within the first two years of public disclosure and likely target their exploits to maximise impact, emphasising the benefit of organisations applying security updates promptly.

In addition to the top 12 list, the advisory also provides technical details about 30 other routinely exploited vulnerabilities, alongside mitigation advice to help organisations and software developers reduce the risk of compromise.

UK organisations are also encouraged to sign up for the NCSC's Early Warning service to receive alerts about potential issues, including vulnerabilities, affecting their networks.

Jonathon Ellison, NCSC Director of Resilience and Future Technology, said:

> "Vulnerabilities are sadly part and parcel of our online world and we see threat actors continue to take advantage of these weaknesses to compromise systems.
>
> "This joint advisory with our allies raises awareness of the most routinely exploited vulnerabilities in 2022 to help organisations identify where they might be at risk and take action.
>
> "To bolster resilience, we encourage organisations to apply all security updates promptly and call on software vendors to ensure security is at the core of their product design to help shift the burden of responsibility away from consumers."

All UK organisations are eligible to sign up for Early Warning and can register via the NCSC website. The NCSC also has guidance to help organisations with vulnerability management.

Software vendors, designers and developers are encouraged to embed secure-by-design practices into every stage of the development life cycle to help identify root causes of vulnerabilities and address them.

The new advisory has been jointly issued by the NCSC, the US Cybersecurity and Infrastructure Security Agency (CISA), the US National Security Agency (NSA), the US Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ) and the New Zealand National Cyber Security Centre (NCSC-NZ).

It can be read on CISA's website.

PUBLISHED

3 August 2023

WRITTEN FOR

Cyber security professionals

Large organisations

Small & medium sized organisations

NEWS TYPE

Alert