

Zero-Day Exploit

A zero-day attacks a software flaw before any patch exists, so the usual advice to update does not help. Here is what a zero-day is, the cases that prove the risk and the controls that limit the damage.

WHAT IT IS

A zero-day exploit attacks a software flaw before the vendor has a patch for it. The name means the vendor has had zero days to fix it, so there is no official defence at the moment the attack begins. It is not only a problem for governments. Flaws in everyday tools like file-transfer software and VPNs have hit thousands of ordinary businesses through the supply chain.

WHY IT MATTERS

21.3%

Of EU intrusions studied began with vulnerability exploitation, second only to phishing.

ENISA, 2025

48,000+

New software vulnerabilities catalogued in 2025, up 22 percent on the year before.

ENISA, 2025

Thousands

Of organisations worldwide were hit through one zero-day in MOVEit Transfer.

CISA and FBI, 2023

WHAT HAPPENED

In May 2023 the CI0p group exploited a previously unknown flaw in MOVEit Transfer, a tool used to move files securely. They stole data from the databases behind it and demanded payment, without ever encrypting a file. A joint CISA and FBI advisory in June 2023 described a campaign that reached thousands of organisations worldwide. (CISA and FBI, 2023)

RED FLAGS TO WATCH FOR

You cannot spot a zero-day by its signature, so watch for behaviour that looks wrong.

- A server suddenly sending large volumes of data to an unfamiliar address.
- A trusted program running commands it never normally runs.
- New accounts or raised privileges on a sensitive system.
- A VPN or security appliance behaving strangely.

THE ONE RULE THAT STOPS IT

Patch internet-facing systems the moment a fix is released, because attackers weaponise disclosed flaws within days.

THEN BUILD THE HABIT AROUND IT

- Keep office systems, servers and any control systems segmented apart.
- Take appliances and services off the public internet where they are not needed.

- Keep a live inventory of the software and components you run.
- Monitor critical systems for unusual behaviour, not just known signatures.

MYTHS AND FACTS

MYTH

Keeping everything patched protects you from zero-days.

FACT

On day zero there is no patch to apply. Defence relies on segmentation, monitoring and fast response instead.

MYTH

Antivirus will catch a zero-day.

FACT

Signature tools only know patterns they have seen. A true zero-day is unknown, so behavioural detection matters more.

MYTH

Zero-days only target big tech and governments.

FACT

Flaws in common tools like MOVEit and Log4j reached thousands of ordinary businesses through the supply chain.

THE LEGAL DUTY

A zero-day that causes a significant incident still triggers duties under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with reporting to MCF (formerly MSB) within 24 and 72 hours and boards personally accountable under Article 20.

GET HELP

eBuilder Security runs managed detection and response that watches for the behaviour a zero-day leaves behind. Read the full guide at the link below.

[Read the Full Article →](#)