z

Zero-Day Attack: Vulnerability, Exploit, Response, and Protection

A zero-day attack exploits a previously unknown vulnerability. Learn the terminology and the response sequence before and after a patch becomes available.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

A **zero-day attack** exploits a hardware, firmware, or software vulnerability that was previously unknown to the vendor or defenders. Because no official fix was available when exploitation began, affected organizations have “zero days” of advance patching time. This matches the NIST definition.

Zero-day vulnerability, exploit, and attack

- A **zero-day vulnerability** is the underlying weakness.
- A **zero-day exploit** is code or a technique that triggers that weakness.
- A **zero-day attack** is actual malicious use of the exploit against a target.

After public disclosure and a vendor fix, the weakness is no longer secret, but unpatched systems remain vulnerable. “Zero-day” does not mean that an attack is undetectable, unstoppable, or automatically the most severe possible threat.

How zero-day attacks are discovered

A researcher may privately report a flaw before anyone sees exploitation. In other cases, defenders find unusual crashes, exploit behavior, malware, or telemetry and trace it to a new vulnerability. The vendor then investigates, assigns an identifier when appropriate, publishes mitigations, and develops a patch.

Ordinary users usually cannot identify a zero-day from symptoms alone. Crashes, slow performance, or an antivirus alert have many causes. Reliable evidence comes from a vendor advisory, incident investigation, exploitation artifacts, or trusted threat intelligence.

What to do before a patch exists

1. **Confirm scope from the vendor.** Identify affected products, versions, configurations, exposure, and prerequisites. Do not rely on an unsourced social-media screenshot.
2. **Inventory affected assets.** Include appliances, embedded components, cloud images, remote devices, and software bundled inside another product.
3. **Apply the published workaround.** Disable the vulnerable feature, restrict network access, remove internet exposure, change a configuration, or use a vendor-provided mitigation exactly as documented.
4. **Add compensating controls.** Segment affected systems, enforce allow-listing, strengthen authentication, restrict attachments or file types, and deploy specific IPS, WAF, EDR, or email rules when validated.
5. **Increase monitoring.** Preserve logs and watch for the behavior and indicators named in the advisory. A block rule reduces risk but does not prove the system was never compromised.

When a patch becomes available

Prioritize internet-facing, privileged, and actively exploited systems. Test for essential compatibility, but do not use routine change windows to postpone an emergency fix without an explicit risk decision.

1. Back up critical configuration and confirm a rollback plan.
2. Install the official update and reboot if required.
3. Verify the installed build, package, or firmware version—not merely that an installer completed.
4. Keep temporary controls until patch coverage and effectiveness are confirmed.
5. Hunt for compromise during the entire possible exposure window. Patching closes the flaw but does not remove an attacker who already gained access.

If exploitation is suspected

Isolate affected systems without destroying evidence, preserve relevant logs and memory when feasible, and activate incident response. Reset exposed credentials only from a known-clean system and after unauthorized persistence is contained. Organizations should follow vendor and government guidance and report material incidents as required.

How to reduce zero-day impact

- maintain accurate asset and software inventories;
- minimize internet exposure and unnecessary features;
- use least privilege, segmentation, application control, and strong authentication;
- centralize logs and deploy behavior-based endpoint and network detection;
- practice emergency patching and incident-response procedures.

Zero-day FAQ

Can antivirus stop a zero-day exploit?

It may block delivery, malicious behavior, or a later payload even without recognizing the vulnerability, but no product guarantees prevention.

Does fully patched mean safe from zero-days?

No. Patching removes known flaws and reduces attack paths, which still limits the damage and options available to an attacker.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com