NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

Zero-Days

What is a zero-day vulnerability?
A zero-day vulnerability is a flaw in software, hardware, or firmware that is unknown except to those that have discovered it. Since no patch or update is available the vulnerability can be exploited by attackers largely without anyone noticing. The term "zero-day" refers to the fact that vendors have had zero-days to address and fix the flaw before it can be maliciously exploited.

Where do zero-days come from?
Like any vulnerability, zero-days often stem from coding errors or design flaws in software that go unnoticed due to the complexity of modern systems and limited security testing. Ethical hackers and researchers typically discover zero-days through testing and responsible disclosure, often incentivized by ethical bug bounty programs. In underground markets, zero-day vulnerabilities are highly valuable, frequently sold by black hat developers to advanced persistent threat (APT) actors for use in malicious campaigns. Additionally, nation-state threat actors invest significant resources into uncovering zero-day vulnerabilities, motivated by cyber espionage, surveillance, or cyber warfare.

How are zero-days exploited?
Once a zero-day vulnerability is discovered, attackers often develop malicious code, such as malware or exploit kits, to exploit the flaw. They frequently use automated tools or bots to scan for publicly accessible or internet-facing systems vulnerable to the zero-day, enabling widespread exploitation. In more targeted attacks, bad actors may conduct reconnaissance to customize their approach, allowing them to penetrate deeper into specific systems or networks.

Why are zero-days so dangerous?
Zero-day vulnerabilities pose a significant risk because they can be exploited before a patch or fix is available, often going undetected for an extended period. Attackers can use zero-days to infiltrate systems, steal sensitive data, disrupt operations, or launch larger cyberattacks.

Since the vulnerability is unknown to the vendor, organizations are left defenseless until the issue is discovered and patched. This window of exposure creates an ideal environment for attackers to cause maximum damage. Once a zero-day vulnerability is publicly exposed it is often heavily exploited by multiple threat actors until mitigation measures are developed.

How can I protect myself or my company?

While it's impossible to predict or completely prevent zero-day attacks, there are steps you can take to reduce the risk:

- Regularly update all software, as security patches and updates often fix known vulnerabilities that may be required in conjunction with new zero-day exploits for a successful attack.
- Implement a multi-layered defense strategy that includes firewalls, intrusion detection/prevention systems, antivirus software, and endpoint protection to reduce the risk of exploitation.
- Use tools that analyze system behavior for anomalies which can help detect zero-day exploits when there are no known malicious signatures.
- Limit user permissions to only what's necessary. This can reduce the spread of damage if a zero-day vulnerability is exploited within your network.
- Having an incident response plan in place ensures that your organization can react quickly to mitigate damage if a zero-day attack occurs.
- Regularly monitor cybersecurity news, advisories, and your technology vendors advisories about emerging vulnerabilities and mitigations.