Cybersecurity Digest

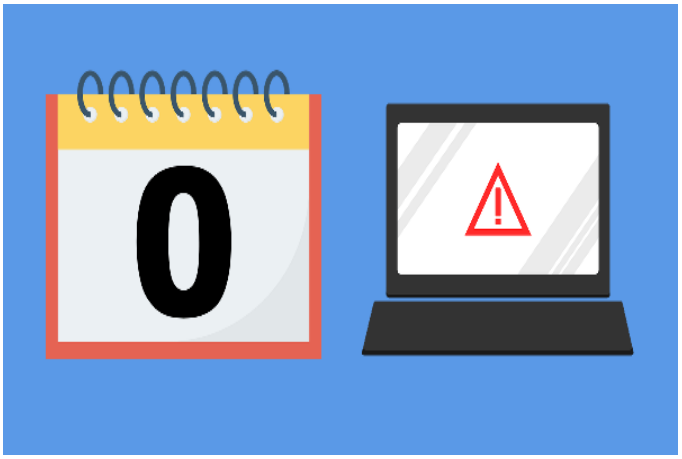
Bi-Weekly update by the O/o CISO of Meghalaya Rural Bank

Volume 3 Issue 8 **Date: 16-07-2026**

Zero Day Attack

A zero day (or 0-day) vulnerability is a security risk in a piece of software that is not publicly known about and the vendor is not aware of. A zero-day exploit is the method an attacker uses to access the vulnerable system. These are severe security threats with high success rates as businesses do not have defenses in place to detect or prevent them.

A zero-day attack is one that is discovered while it is already in progress, meaning a security team has "zero days" to prepare or remediate the vector through which the attacker gained entry.



How a zero day exploit works

A zero day attack begins with a software developer releasing vulnerable code that is spotted and exploited by a malicious actor. The attack is then either successful, which likely results in the attacker committing identity or information theft, or the developer creates a patch to limit its spread. As soon as a patch has been written and applied, the exploit is no longer referred to as a zero day exploit.

The timeline of zero day exploitation has been split into seven separate stages by security researchers Leyla Bilge and Tudor Dumitras from vulnerability introduction to security patch. They are as follows:

1 Vulnerability introduced: A developer creates software that, without them realizing, contains vulnerable code.

2. Exploit released: A malicious actor discovers the vulnerability before the developer realizes it exists or before they have been able to fix or patch it. The hacker then writes and deploys an exploit code while the vulnerability is still open.

3. Vulnerability discovered: The vendor becomes aware of the vulnerability but does not have a patch available.

4. Vulnerability disclosed: The vendor and/or security researchers announce the vulnerability publicly, which advises users and attackers of its existence.

5. Antivirus signatures released: If attackers have created zero day malware targeting the vulnerability, then antivirus vendors can quickly identify its signature and provide protection against it. However, systems may remain exposed if there are other ways of exploiting the vulnerability.

6. Security patch released: The vendor releases a public fix to close the vulnerability. How long this takes to arrive depends on the complexity and how much of a priority it takes in their development process.

7. **Security patch deployment completed**: Releasing a security patch does not provide an instant fix as it can take time for users to deploy it. For this reason, organizations and individual users should switch on automatic software updates and take notice of update notifications.

Systems are vulnerable to attack through the entire process from stages 1 to 7, but a zero day attack can only occur between stages 2 and 4. Further attacks can occur if the vulnerability remains unprotected. Zero day attacks are rarely discovered quickly enough to prevent substantial damage. It can typically take days, months, and even years before a developer realizes the vulnerability existed and led to an attack and data breach.

Zero day threat examples

A zero day attack can happen to any company at any time, often without them realizing. High-profile examples of zero-day attacks include:

Sony Pictures: Potentially the most famous zero day attack took down the Sony network and led to the release of its sensitive data on file-sharing sites. The attack, in late 2014, saw the leak of information around upcoming movies, the company's business plans, and personal email addresses of senior executives.

RSA: Another highly public zero day attack saw hackers use an unpatched vulnerability in Adobe Flash Player to gain access to the network of security firm RSA in 2011. The attackers sent emails attached with Excel spreadsheets, which contained an embedded Flash file that exploited the zero-day vulnerability, to RSA employees. When employees opened the spreadsheet, it gave the attacker remote control of the user's computer, which they used to search for and steal data. That information turned out to be related to its SecurID two-factor authentication products that employees use to access sensitive data and devices.

Operation Aurora: In 2009, a zero day exploit targeted the intellectual property of more than 20 major global organizations, including Adobe Systems, Blackberry, Dow Chemical, Google, Morgan Stanley, and Yahoo. It exploited vulnerabilities in Internet Explorer, various other Windows software versions, and Perforce, which Google used to manage its source code. The attack aimed to gain access to and modify source code repositories at high-tech organizations.

How to protect against zero day attacks?

Vulnerability scanning

Solutions that scan for vulnerabilities can simulate attacks on software code, review code for errors, and attempt to find new issues that have been introduced in a software update. However, this approach will not detect all zero-day exploits, and scanning alone is not enough. Businesses need to act quickly on the results of a scan and review code to prevent an exploit.

Patch management

Patch management: Deploying software patches as soon as possible after discovering a software vulnerability can reduce the risk of an attack. However, it cannot prevent an attack if the hacker creates their exploit quicker than the patch is deployed. The longer the patch process takes, the higher the risk of a zero-day attack occurring.

Stay informed

Being proactive and staying informed on the latest risks in the threat landscape is a vital first step in preventing zero day attacks.

This includes deploying comprehensive security software that will block known and unknown threats, supported by anomaly detection using machine learning models to uncover previously unseen attack patterns. It also includes employees practicing safe and secure online habits and configuring security settings for their browsers and systems.

Perform system updates

Ensuring systems are up to date is crucial to protecting a business from the risk of zero day attacks. This includes having the latest features installed, removing outdated or defunct features, updating drivers, fixing bugs, and filling potential holes in security.

Use a next-generation firewall

Traditional antivirus software cannot effectively protect businesses from zero day threats. Instead, businesses need to look for solutions that block unknown zero-day malware.