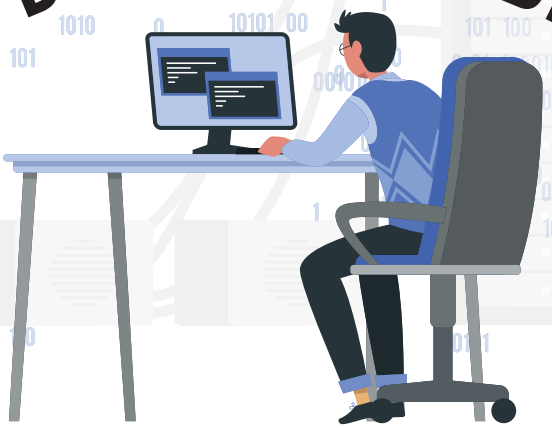
ZERO DAY VULNERABILITIES



In the world of cybersecurity, there are many threats that force organizations to be in a constant defensive stance. Unfortunately, regardless of the efforts people put into protecting data and systems, there's one particular threat that can easily override those efforts: the zero-day vulnerability.

WHAT IS A ZERO-DAY VULNERABILITY?

A zero-day vulnerability is a flaw in software that is discovered by cybercriminals before the software developer is aware of the flaw. It's referred to as a "zero-day" because once it's discovered, the developer has zero days to issue a fix before attackers exploit the vulnerability.

WHAT IS A ZERO-DAY EXPLOIT?

The zero-day exploit is the process of attacking the vulnerability after it's discovered. Cybercriminals can carry out numerous attacks using the exploit, such as stealing data, infecting systems with malicious software (malware), and gaining remote access to devices.

ARE ZERO-DAYS ALWAYS DISCOVERED BY CYBERCRIMINALS FIRST?

Thankfully, no. There are many "good hackers" around the world who often discover vulnerabilities and immediately report them to the appropriate party. In some cases, those scenarios can result in a cash reward for the discovery. But many vulnerabilities are, unfortunately, first discovered by criminals.

HOW CAN ORGANIZATIONS AVOID ZERO-DAY VULNERABILITIES?

Due to the nature of these flaws and the way they're exploited, it can be incredibly difficult to defend against them. There are, however, a few actions organizations and individuals can take to protect themselves:

- **KEEP ALL SOFTWARE AND DEVICES UP TO DATE.**
  Many zero-day vulnerabilities exist in outdated software that effectively leaves a backdoor open for cybercriminals. By running updates and keeping systems and devices current, organizations can at least avoid those types of threats.
- **REMOVE UNUSED SOFTWARE.**
  Over time, computers and mobile devices tend to have several programs installed that are no longer needed or rarely used. This usually means that the programs remain outdated and vulnerable to cyberattacks. It's always a good idea to occasionally audit systems and devices to remove unneeded software.
- **IMPLEMENT MODERN SOFTWARE SOLUTIONS.**
  It's vital to monitor networks to identify unusual activity. There are many software solutions for this process that utilize modern concepts, such as machine learning and artificial intelligence. It's also important to stay informed about the latest cybersecurity threats and known attacks.
- **REPORT ANYTHING SUSPICIOUS IMMEDIATELY.**
  While employees across an organization might not be in a position to influence cybersecurity strategies, every individual should report suspicious activities immediately. Timely reporting empowers security teams and IT personnel to quickly assess an incident and remediate it, thereby reducing potential damages.