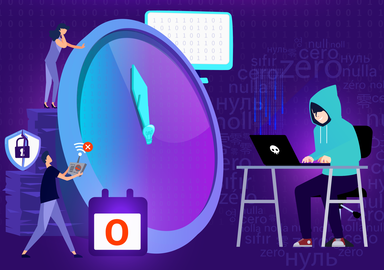
ManageEngine
Vulnerability Manager Plus

ZERO-DAY 101



DECIPHERING 0-DAY ATTACKS

Zero-day vulnerabilities → Zero-day exploits → Zero-day attacks

WHAT IS A ZERO-DAY VULNERABILITY?

The mysterious software flaw that arises without the knowledge of the software vendor is known as zero-day vulnerability. These types of security vulnerabilities do not have patches readily available.

WHY DO WE USE THIS NAME?

Organizations utilize zero-day patches to secure their system from this type of vulnerability and vendors have "zero-days" to develop patches for the same. Without proper mitigation strategies, this zero-day vulnerability can later segue into a major cyberattack.

WHAT ARE ZERO-DAY ATTACKS?

When the zero-day vulnerability is exploited because of the unavailability of patches, it leads to a zero-day attack.

HOW DO YOU PREVENT ZERO-DAY VULNERABILITIES FROM BEING EASILY BYPASSED?

1. Ensure vulnerability scanners are in place
2. Install applicable patches in a timely manner
3. Have a workaround mitigation plan available

WHY ARE ZERO-DAYS CONSIDERED DANGEROUS?

Hidden flaws: These vulnerabilities can be exploited for a longer time before they are discovered.

Polymorphic: This malware from zero-day exploits can be developed to attack continuously and evade detection.

Penetrative: A zero-day attack can infiltrate multiple systems in a network.

ZERO-DAY ATTACKS THAT LEFT A MAJOR IMPACT IN 2023

ZERO-DAY ATTACK IN WORDPRESS

A zero-day exploit in a plug-in with 200k users helped hackers bypass protection by enabling them to gain administrative privileges.

Source: SecurityWeek

CRYPTOCURRENCY STOLEN VIA A SINGLE ZERO-DAY SECURITY FLAW

Around 1.6 million in cryptocurrency has been reportedly stolen due to an active zero-day exploit in General Bytes Bitcoin ATM.

Source: TheHackerNews

HITACHI ENERGY ATTACKED BY RANSOMWARE DUE TO A CRITICAL ZERO-DAY VULNERABILITY.

This zero-day vulnerability was found in a third-party software that was leveraged by the CLOP ransomware gang. They have reportedly stolen the organization's data from the cloud servers of the third-party software.

Source: BleepingComputer

ZERO-DAY VULNERABILITIES FIXED BY REPUTED VENDORS IN H1 OF 2023

Number of zero-day vulnerabilities fixed in **Chrome**

10

Number of zero-day vulnerabilities fixed in **Microsoft**

55

THE SOLUTION TO SEAMLESSLY DETECT AND MITIGATE VULNERABILITIES?

ManageEngine Vulnerability Manager Plus changes your vulnerability detection game by swiftly spotting zero-day vulnerabilities and remediating them with workarounds —before they are exploited.

DOWNLOAD NOW

Protect Endpoints, Prevent Cyberattacks