Zero-Day Vulnerabilities and Zero-Day Attacks

March 3, 2021

Every now and then, a zero-day attack will make headlines in the world of cybersecurity. Zero-day attacks exploit zero-day vulnerabilities. According to Ryan Naraine of ZDNet, the Stuxnet worm—discovered in 2020—used four zero-day vulnerabilities. The Stuxnet worm is famous for damaging Iran's nuclear infrastructure. Another famous example would be the Sony Pictures hack in 2014. According to Arik Hesseldahl of Vox, this hack involved a zero-day attack. Recently, on February 2, 2021, the Cybersecurity and Infrastructure Intelligence Agency (CISA) reported a zero-day vulnerability in SonicWall SMA 100 Series Version 10.x products. On February 22, 2021, the cybersecurity firm FireEye reported that "multiple zero-day vulnerabilities in Accellion's legacy File Transfer Appliance (FTA)" were exploited by bad actors known as UNC2546 for the purpose of cyber extortion—stealing data and threatening to publish it unless a ransom is paid, typically an application of ransomware. However, you may wonder about what zero-day vulnerabilities and zero-day attacks actually are, and why they are so damaging. This article contains some terms and definitions to help you get up to speed.

A vulnerability is a flaw. Specifically, it is a flaw within software, firmware, or even hardware that can be exploited by a bad actor. To exploit a vulnerability is to use the flaw in order to accomplish some goal. Oftentimes, vulnerabilities are exploited by inserting code into something or sending messages with specific

values. One example of a software vulnerability would be GUI code for an SQL database that does not properly sanitize the data that is inserted by a user—that is, it does not ensure that user input is a valid query. In an SQL injection attack, the attacker exploits this vulnerability by inserting arbitrary code as input. Because the input is not sanitized, the arbitrary code is executed. The arbitrary code may be written to do anything the attacker wants, such as reveal all the secret data in the database, or even delete everything.

Zero-day attack is a loose term. According to the National Institute of Standards and Technology (NIST), a zero-day attack is "[a]n attack that exploits a previously unknown hardware, firmware, or software vulnerability." Normal vulnerabilities are publicly known to exist within certain products and services. They can be detected by cybersecurity software and cybersecurity professionals. Once detected, they can be mitigated. Unknown vulnerabilities are also referred to as zero-day vulnerabilities, and they are very hard to mitigate precisely because they are unknown. Antivirus software does not know to look for them, so the victims are completely unaware that they can be attacked until it is too late. This element of surprise is what makes zero-day attacks particularly dangerous.

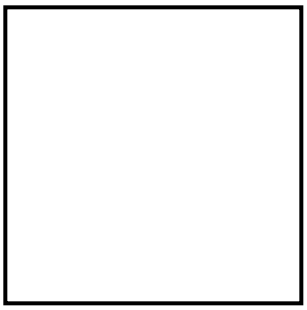
Whether vulnerabilities are zero-day vulnerabilities depends on whether they are unknown to the victim and their defenses. They could either be unknown to a particular victim, or they could be unknown to the general public. As mentioned in a previous blog article, the National Security Agency (NSA) would sometimes keep vulnerabilities a secret from the general public. These vulnerabilities were zero-day vulnerabilities to the general public, but they were known vulnerabilities to the NSA.

There is a different definition of "zero-day attack" that is less general than the NIST definition. According to FireEye, a zero-day attack occurs when a previous unknown vulnerability is found and exploited "before a developer has an opportunity to create a patch to fix the vulnerability." Before a patch is released, an attacker may write exploit code to be used for attacks. However, "[o]nce a patch is written and used, the exploit is no longer called a zero-day exploit," and attacks that exploit the vulnerability are no longer zero-day attacks. Under this definition, whether an attack is a zero-day attack depends on whether the code of the vulnerable software has been fixed by developers. This definition is software-specific, whereas the NIST definition applies to firmware and hardware too.

It is actually possible to detect zero-day attacks by looking for behavior that is suspicious. An Intrusion Detection System (IDS) monitors events on a computer or network in order to identify intrusions. Traditional antivirus software and Signature-based Intrusion Detection Systems look for specific signatures, patterns of information that can identify attacks. Using signatures to identify attacks is a bit like using fingerprints to identify criminals. Zero-day attacks do not have signatures, so they have to be identified based on how they are interacting with the targeted system. An Anomaly-based IDS looks for events that are unusual

compared to the events that happen on the computer or network every day. An anomalous event could be a user logging in at a time that is inconsistent with their daily routine, or a program that is suddenly using far more computing resources than usual. An Anomaly-based IDS can detect a zero-day attack because it can detect the suspicious behavior associated with the attack. Runtime Application Self-Protection (RASP) is technology that can detect and prevent zero-day attacks. RASP inspects the data being given to an application as input and checks to see if it leads to any unsafe results, and blocks inputs that lead to these results.

In summary, a zero-day attack is one that exploits an unknown vulnerability. Zero-day attacks are severe because they exploit vulnerable code before a patch is released, so software updates will not help, although they do reduce the risk of newly discovered vulnerabilities being exploited. Zero-day attacks cannot be detected by security software that relies on signatures. Instead, they have to be prevented by using technology that identifies suspicious events.



Evan Mulloy

Associate Software Developer at SD Solutions LLC

Evan Mulloy has been a passionate programmer since the age of 12. He enjoys coding in a wide variety of languages, as well as studying new concepts related to computer science and cybersecurity.

CISA, cyber extortion, cybersecurity, exploitation, hack, NIST, Stuxnet, vulnerabilities, vulnerability, worm, zero-day

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

Post Comment

Recent Posts

Reducing the Significant Risk of Known Exploited Vulnerabilities with IT Asset and Vulnerability Management

Cybersecurity Awareness Month 2021 Week 2: Phight the Phish!

Cybersecurity Awareness Month 2021 Week 1

Health Workforce Data Visualizations get Published for Public Use

SD Solutions wins 5-year contract from AHRQ

Categories

Collaboration

Cybersecurity

News

Technology

Archives

November 2021

October 2021

September 2021

August 2021

July 2021

June 2021

May 2021

April 2021

March 2021

February 2021

January 2021

December 2020

November 2020

October 2020

September 2020

August 2020

July 2020

June 2020

May 2020

April 2020

March 2020

February 2020

January 2020

December 2019

September 2019

September 2018

August 2018

July 2018

June 2018

May 2018

September 2017

July 2017

June 2017

May 2016

April 2016