

CS 419: Computer Security

Week 1: Part 2

Threats, Vulnerabilities, & Attacks



Paul Krzyzanowski

© 2022-2025 Paul Krzyzanowski. No part of this content may be reproduced or reposted in whole or in part in any manner without the permission of the copyright owner.

Definitions

Vulnerability

A weakness in the implementation or operation of a system that can be exploited: a bad policy or a bug

Exploit

Software, commands, or instructions to take advantage of a vulnerability

Attack Vector

The type of attack – the technique that's used to attack the system (e.g., email attachment, network, website)

Attack (cyberattack)

The active use of an exploit via the attack vector to subvert security policies and mechanisms

Threat

The possibility of an attack

Threat Actor

The agent who may carry out the attack

Attack surface

All possible entry points in the system – all the attack vectors in the system

We need to be aware of the attack surface of an environment

- Otherwise, we don't know what to defend
- If possible, **reduce the attack surface**: that way, there will be less we need to protect

Vulnerabilities

- **Failures in the system: policies or mechanisms**
- **Bugs**
- **Big focus in security classes**

Some vulnerabilities can be really old

CISA Adds Five-Year-Old jQuery XSS Flaw to Exploited Vulnerabilities List

The Hacker News

Ravie Lakshmanan • Jan 24, 2025

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday placed a now-patched security flaw impacting the popular jQuery JavaScript library to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.

The medium-severity vulnerability is CVE-2020-11023 (CVSS score: 6.1/6.9), a nearly five-year-old cross-site scripting (XSS) bug that could be exploited to achieve arbitrary code execution.

"Passing HTML containing <option> elements from untrusted sources - even after sanitizing them - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code," according to a GitHub advisory released for the flaw.

<https://thehackernews.com/2025/01/cisa-adds-five-year-old-jquery-xss-flaw.html>

Some vulnerabilities can be really old

16-Year-Old HP Printer-Driver Bug Impacts Millions of Windows Machines



The bug could allow cyberattackers to bypass security products, tamper with data and run code in kernel mode.

Tara Seals • July 20, 2021

Researchers have released technical details on a high-severity privilege-escalation flaw in HP printer drivers (also used by Samsung and Xerox), which impacts hundreds of millions of Windows machines.

If exploited, cyberattackers could bypass security products; install programs; view, change, encrypt or delete data; or create new accounts with more extensive user rights.

The bug (CVE-2021-3438) has lurked in systems for 16 years, researchers at SentinelOne said, but was only uncovered this year. It carries an 8.8 out of 10 rating on the CVSS scale, making it high-severity.

<https://threatpost.com/hp-printer-driver-bug-windows/167944/>

Some vulnerabilities can be really old

Hack Brief: Microsoft Warns of a 17-Year-Old ‘Wormable’ Bug



The SigRed vulnerability exists in Windows DNS, used by practically every small and medium-sized organization in the world.

Andy Greenberg • July 14, 2020

Since Wannacry and NotPetya struck the internet just over three years ago, the security industry has scrutinized every new Windows bug that could be used to create a similar world-shaking worm. Now one potentially "wormable" vulnerability—meaning **an attack can spread from one machine to another with no human interaction**—has appeared in Microsoft's implementation of the domain name system protocol, one of the fundamental building blocks of the internet.

As part of its Patch Tuesday batch of software updates, Microsoft today released a fix for a bug discovered by Israeli security firm Check Point, which the company's researchers have named SigRed. **The SigRed bug exploits Windows DNS, one of the most popular kinds of DNS software that translates domain names into IP addresses.** Windows DNS runs on the DNS servers of practically every small and medium-sized organization around the world. The bug, Check Point says, has existed in that software for a remarkable 17 years.

Check Point and Microsoft warn that **the flaw is critical, a 10 out of 10 on the common vulnerability scoring system**, an industry-standard severity rating.

Chrome, Safari and other browsers vulnerable to 0.0.0.0 Day vulnerability — what you need to know

This critical vulnerability laid **dormant for 18 years** but can now be used by hackers in their attacks

Anthony Spadafora • August 8, 2024

It's not every day that we come across a vulnerability that's almost two decades old but cybersecurity researchers have discovered a new zero-day flaw that impacts all major browsers.

As reported by The Hacker News, the Israeli app security firm Oligo found what it's calling a "0.0.0.0 Day" that can be exploited by hackers to access sensitive services running on local devices. The most surprising thing about this critical vulnerability though is that it has laid dormant in popular browsers for 18 years.

The 0.0.0.0 Day impacts all of the top browsers including Google Chrome and other Chromium-based browsers like Edge, Safari and Firefox. However, it's worth noting that it only affects devices running macOS and Linux. The reason why the best Windows laptops aren't affected is due to the fact that Microsoft blocks this IP address at the operating system level.

<https://www.tomsguide.com/computing/online-security/chrome-safari-and-other-browsers-vulnerable-to-0000-day-vulnerability-what-you-need-to-know>

Lots of systems aren't updated

Hackers are using this old trick to dodge security protections



CVE-2015-2291 is a years-old security vulnerability - but cyber criminals are still able to take advantage of unpatched systems to compromise networks.

Danny Palmer • January 13, 2023

Cyber criminals are exploiting an old vulnerability in Intel drivers in an attempt to gain access to networks in a way that allows them to bypass cybersecurity protections.

...

Once inside a network, Scattered Spider uses a technique that CrowdStrike describes as 'Bring Your Own Vulnerable Driver' (BYOVD), which targets loopholes in Windows security.

While Microsoft attempts to limit the capabilities of malware gaining access to systems by preventing unsigned kernel-mode drivers to be run by default, attackers can get around this with BYOVD, which enables them to install a legitimately signed but malicious driver to carry out attacks.

...

One of the ways they do this operation as stealthily as possible is by not using malware, but instead installing a range of legitimate remote access tools to ensure persistence on the compromised system.

According to analysis by CrowdStrike, the attackers are delivering malicious kernel drivers through a vulnerability in the Intel Ethernet diagnostics driver for Windows (tracked as CVE-2015-2291).

<https://www.zdnet.com/article/hackers-are-using-this-old-trick-to-dodge-security-protections/>

Russian Hackers Hitting Critical Infrastructure, FBI Warns

State-Sponsored Espionage Group Tied to Exploits of No-Longer-Supported Cisco Gear

Matthew J. Schwartz • August 21, 2025

Russian intelligence hackers are using obsolete and unpatched equipment made by networking mainstay Cisco Systems to further stealthy and ongoing cyberespionage operations, the U.S. federal government warned Wednesday.

The FBI in an advisory report said hackers from the Federal Security Service - the FSB, the Russian successor to the KGB - are targeting the United States and allies IT and operational technology environments.

For at least the past year, the hackers have been "collecting configuration files for thousands of networking devices associated with U.S. entities across critical infrastructure sectors" and using the files to gain authorized access to the networking equipment, the bureau said. "The actors used the unauthorized access to conduct reconnaissance in the victim networks, which revealed their interest in protocols and applications commonly associated with industrial control systems."

The U.S. government attributes the attacks to an FSB unit known as Center 16. The group exploits a vulnerability in the Smart Install feature of Cisco devices, tracked as CVE-2018-0171, which attackers can use to execute arbitrary code on a device.

<https://www.govinfosecurity.com/russian-hackers-hitting-critical-infrastructure-fbi-warns-a-29268>

Lots of systems aren't updated

Nation state hackers exploited years-old bug to breach a US federal agency



Carly Page • March 16, 2023

The U.S. government has warned that multiple cybercriminal gangs, including a nation state-backed hacking group, exploited a four-year-old software vulnerability in order to compromise a U.S. federal government agency.

A joint alert released by the CISA, the FBI and the Multi-State Information Sharing and Analysis Center (known as MS-ISAC) on Wednesday revealed that hackers from multiple hacking groups exploited known vulnerabilities in Telerik, a user interface tool for web servers. This software — designed for building components and themes for web applications — was running on the U.S. agency's internet-facing web server.

<https://techcrunch.com/2023/03/16/cisa-nation-state-hackers-breach-federal-agency/>

Lots of systems aren't updated

10-year-old Windows bug with 'opt-in' fix exploited in 3CX attack

BLEEPINGCOMPUTER

Carly Page • March 16, 2023

A 10-year-old Windows vulnerability is still being exploited in attacks to make it appear that executables are legitimately signed, with the fix from Microsoft still "opt-in" after all these years. Even worse, the fix is removed after upgrading to Windows 11.

On Wednesday night, news broke that VoIP communications company 3CX was compromised to distribute trojanized versions of its Windows desktop application in a large-scale supply chain attack.

As part of this supply chain attack, two DLLs used by the Windows desktop application were replaced with malicious versions that download additional malware to computers, such as an information-stealing trojan.

One of the malicious DLLs used in the attack is usually a legitimate DLL signed by Microsoft named d3dcompiler_47.dll. However, the threat actors modified the DLL to include an encrypted malicious payload at the end of the file.

As first noted yesterday, even though the file was modified, Windows still showed it as correctly signed by Microsoft.

<https://www.bleepingcomputer.com/news/microsoft/10-year-old-windows-bug-with-opt-in-fix-exploited-in-3cx-attack/>

Vulnerabilities are on the rise: 2023 beats 2022

Majority of 2023's critical cyberattacks stemmed from fewer than 1% of vulnerabilities

Duncan Riley • December 19, 2023



There were 26,447 vulnerabilities discovered in 2023, surpassing the number of vulnerabilities disclosed in 2022 by more than 1,500 and the highest number ever disclosed. Of the disclosed vulnerabilities, more than 7,000 had proof-of-concept exploit code that could potentially result in successful exploitation. But the exploit code was typically of lower quality, which may reduce the likelihood of a successful attack.

Some 206 vulnerabilities had weaponized exploit code available, meaning they were highly likely to compromise the target system if used. There were 115 vulnerabilities that were routinely exploited by threat actors, malware and ransomware groups such as Clon.

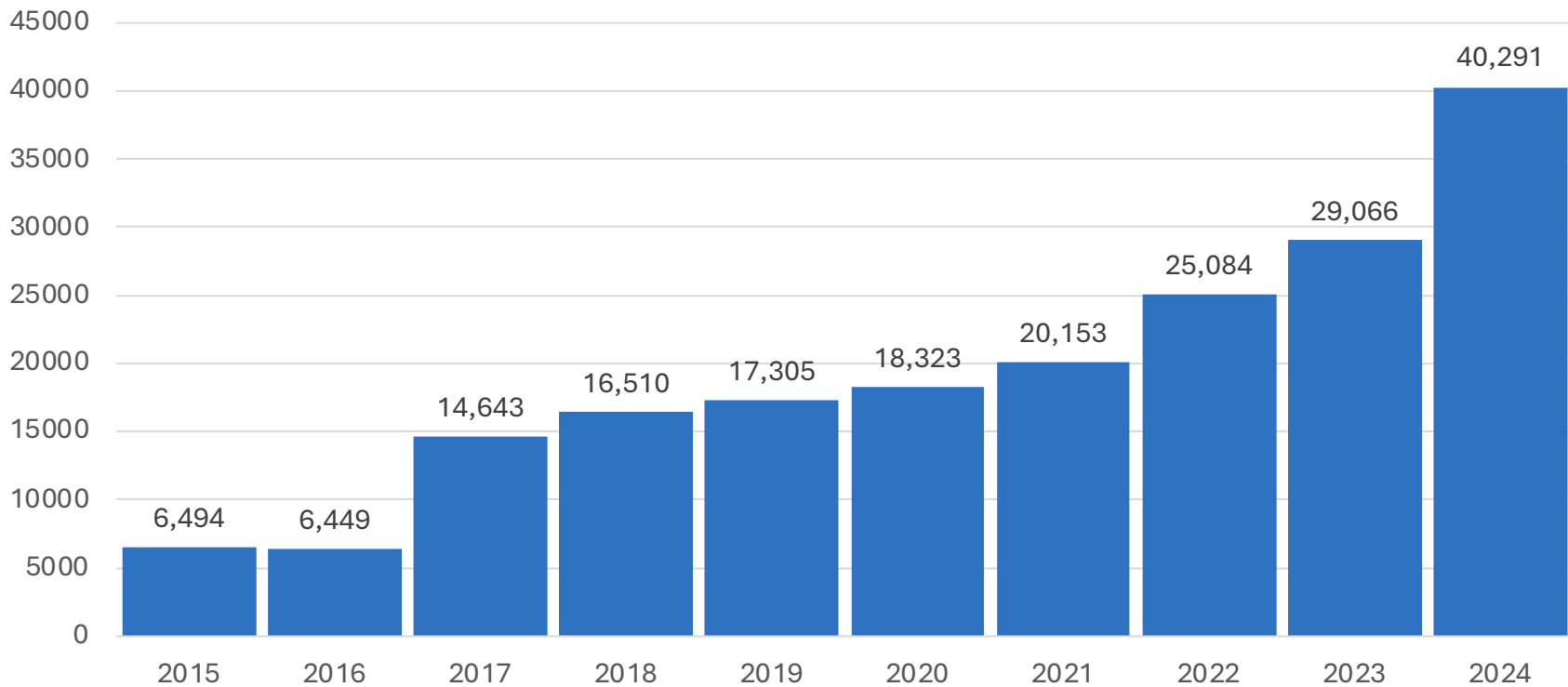
More than a third of the identified high-risk vulnerabilities identified could be exploited remotely. The five most prevalent types of vulnerabilities comprised over 70% of the total discovered.

The mean time to exploit high-risk vulnerabilities in 2023 came in at about 44 days. However, the report notes that in numerous instances, exploitation occurred almost instantaneously, with some vulnerabilities exploited on the very day they were published.

<https://siliconangle.com/2023/12/19/majority-2023s-critical-cyber-attacks-stemmed-less-1-vulnerabilities/>

Vulnerabilities 2015 – 2024

Published Vulnerabilities



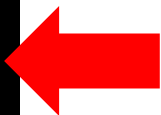
Data from <https://www.cvedetails.com/browse-by-date.php>

People Make Mistakes

January 2025: DNS configuration error at MasterCard Present for almost five years!

```
;; AUTHORITY SECTION:
az.mastercard.com.      3600      IN        NS        a1-29.akam.net.
az.mastercard.com.      3600      IN        NS        a7-67.akam.net.
az.mastercard.com.      3600      IN        NS        a22-65.akam.ne.
az.mastercard.com.      3600      IN        NS        a26-66.akam.net.
az.mastercard.com.      3600      IN        NS        a9-64.akam.net.

;; Query time: 92 msec
;; SERVER: 216.119.218.53#53(dnsl.mastercard.com) (TCP)
;; WHEN: Fri Jan 10 11:24:51 EST 2025
;; MSG SIZE rcvd: 191
```



<https://krebsonsecurity.com/2025/01/mastercard-dns-error-went-unnoticed-for-years/>

Threat categories

- **Disclosure: Unauthorized access to data**
 - Snooping (wiretapping)
- **Deception: Acceptance of false data**
 - Injection of data, modification of data, denial of receipt
- **Disruption: Interruption or prevention of correct operation**
 - Denial of service, data deletion, or modification
- **Usurpation: Unauthorized control of some part of a system**
 - May lead to modification, spoofing, delay, denial of service

Possible Attacks

- **Snooping: unauthorized interception of information**
 - Form of disclosure
 - Counter with confidentiality services
- **Modification or alteration: unauthorized change of information**
 - Form of deception, disruption or usurpation
 - Counter with integrity services
- **Masquerading or spoofing: impersonation of one entity by another**
 - Form of deception and usurpation
 - Counter with integrity services
- **Repudiation of origin: false denial that an entity sent or created something**
 - Form of deception and usurpation
 - Counter with integrity services

Possible Attacks

- **Denial of receipt: false denial that an entity received data or a message**
 - Form of deception
 - Counter with integrity & availability mechanisms
- **Delay: temporary inhibition of a service**
 - Form of disruption (possibly via usurpation)
 - Counter with availability mechanisms
- **Denial of service: long-term inhibition of a service**
 - Form of disruption (possibly via usurpation)
 - Counter with availability mechanisms

Threats

Protection: Know Your Enemy!

Different attackers

... have different goals

... and different skill levels



“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, The Art of War

Who do we want to – or need to – guard against?

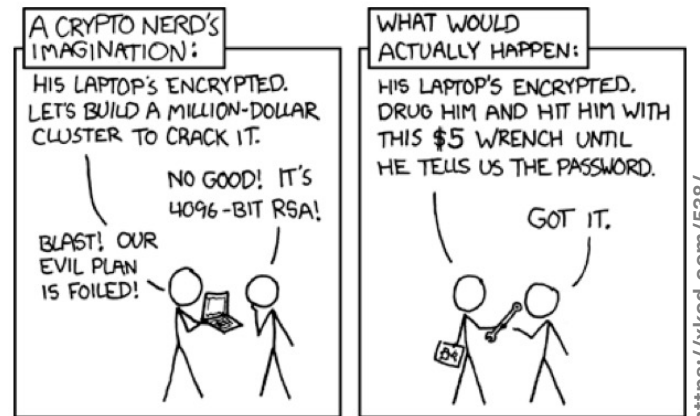
What are you securing your system against?

And from whom?

- You accidentally deleting important system files?
- Your colleagues not being able to look at your files on a file server?
- A company trying to find out about you and get personal data?
- A phone carrier tracking your movement?
- A grenade destroying your system?
- Video surveillance on streets?
- The NSA?

Who are the potential attackers?

- Who are the adversaries?
- Lot of variations
- Different attackers have different abilities
- Are enemies sufficiently motivated to attack you?
- Attackers can often resort to the **three Bs: Burglary, Bribery, or Blackmail**



Coinbase says cyberattack cost up to \$400 million after bribed overseas employees stole customer data

MarketWatch

Crypto-trading company said clients were already informed of the breach, which may cost it up to \$400 million based on current estimates.

By Steve Gelsi | May 15, 2025

Coinbase Global Inc. said Thursday it's working with law enforcement to track down an unknown "threat actor" that paid its contractors working in support roles for the company outside the U.S. to obtain personal information about its customer base.

Coinbase did not say how many of its clients were affected, but it had already informed them about the breach after it detected it months ago and fired the contractors involved.



"The threat actor appears to have obtained this information by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems to which they had access in order to perform their job responsibilities," the company said.

<https://www.marketwatch.com/story/coinbase-suffers-cyber-attack-as-oversees-employees-were-bribed-to-steal-customer-data-c74b2840>

AT&T employees took bribes to plant malware on the company's network



DOJ charges Pakistani man with bribing AT&T employees more than \$1 million to install malware on the company's network, unlock more than 2 million devices.

By Catalin Cimpanu for Zero Day | August 6, 2019 -- 14:02 GMT (07:02 PDT) | Topic: Security



AT&T employees took bribes to unlock millions of smartphones, and to install malware and unauthorized hardware on the company's network, the Department of Justice said yesterday.

These details come from a DOJ case opened against Muhammad Fahd, a 34-year-old man from Pakistan, and his co-conspirator, Ghulam Jiwani, believed to be deceased.

SIM Swappers Try Bribing T-Mobile and Verizon Staff \$300

DOJ charges Pakistani man with bribing AT&T employees more than \$1 million to install malware on the company's network, unlock more than 2 million devices.

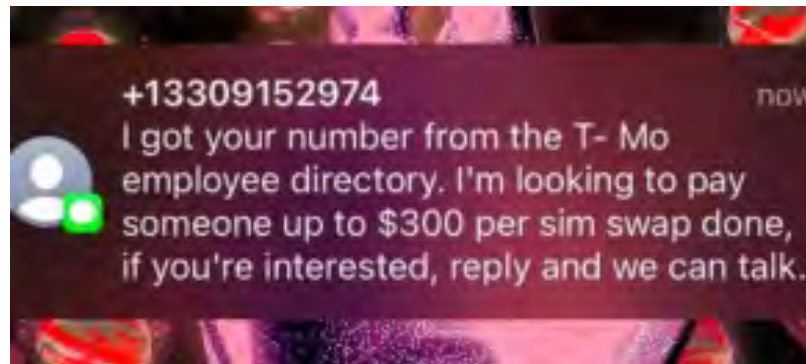
By Richi Jennings | April 16, 2024

It's no secret that cellular carrier reps are subject to bribery. Here's a great example. Yes, again with the SIM swapping—where a fraudster convinces a representative to move a target's line to a new SIM because they “lost” their phone.

Someone seems to have stolen a contact list of

T-Mobile employees and is texting them offers of bribes to execute SIM swaps. But T-Mobile denies it's been hacked... again.

Here's the soft underbelly of the insider threat model. In today's SB Blogwatch, we balk at the three-Benjamin bribes.



July 2020 Twitter (X) Breach

- **Hackers targeted 130 users**
- **Tweeted cryptocurrency scam from 45 accounts they were able to access**
 - Changing the email address & login credentials
- **Brought in \$120,000**
- **Not a big deal ... but could have been a lot worse**
 - X is used by political & business leaders
 - The right tweet can move markets or start conflicts



What happened?

Internal employee changed email addresses and turned off security features of certain high-profile accounts.

It wasn't social engineering, it was bribery — a Twitter employee was paid.

Insider threat problem: Twitter had almost 5,000 employees at the time.



<https://www.theverge.com/2020/7/15/21326656/twitter-hack-explanation-bitcoin-accounts-employee->

Exclusive: More than 1,000 people at Twitter had ability to aid hack of accounts



Joseph Menn, Katie Paul, Raphael Satter • July 23, 2020

SAN FRANCISCO (Reuters) - More than a thousand Twitter employees and contractors as of earlier this year had access to internal tools that could change user account settings and hand control to others, two former employees said, making it hard to defend against the hacking that occurred last week.

Twitter said on Saturday that the perpetrators "manipulated a small number of employees and used their credentials" to log into tools and turn over access to 45 accounts. here On Wednesday, it said that the hackers could have read direct messages to and from 36 accounts but did not identify the affected users.

The former employees familiar with Twitter security practices said that too many people could have done the same thing, more than 1,000 as of earlier in 2020, including some at contractors like Cognizant.

<https://www.reuters.com/article/us-twitter-cyber-access-exclusive/exclusive-more-than-1000-people-at-twitter-had-ability-to-aid-hack-of-accounts-idUSKCN24O34E>

Threat Models

- **Set of assumptions about the abilities of an adversary**
- **A way to identify & prioritize potential threats from an attacker's point of view**
 - Think about things that could go wrong
 - Bad guys don't follow rules: they don't care about your policies
 - We need to understand what types of attacks are possible
- **Assess**
 - What's valuable?
 - Where will you be likely to be attacked?
 - What are the most significant threats?
- **Think about entities in the system, how they communicate & store data**
 - Where are the trust boundaries?
 - Where and how is protection enforced?

The End