

Cat’s Company’s Holes Revealed

By: Curtis Crawford



July 24, 2023

Lighthouse Labs

Cyber Security Flex

Executive Summary

The scans and reports conducted in this report are to identify and prioritize the vulnerabilities of Cat’s systems. This will improve the security weaknesses, strengthen the security posture, and help grow the networking environment of the organisation. The scanning software that was used to assist in this process was the OpenVAS tool. The systems belonging to Cat’s that were under evaluation were the Windows 1 Machine, Windows Server, and Linux Server. During these scans, a number of vulnerabilities were revealed. I have ranked and specified, according to their CVSS score and impact (with a maximum threat score of 10), which of these vulnerabilities are most critical. These vulnerabilities are as follows:

Windows Remote Desktop Licensing Service (CVE-2024-38077)

Windows Internet Key Exchange Protocol Extensions (CVE-2022-34722)

Microsoft Windows Support Diagnostic Tool (MSDT) (CVE-2023-36911 and CVE-2022-30190)

Such vulnerabilities will be explained more thoroughly in this report but it should be briefly stated for your understanding that they are serious because they can open the door to the worst of all worlds. Things including stealing data, taking control of systems, and disrupting services. Not to worry, these vulnerabilities can be addressed with patches and updates to the system configurations. Along with these fixes, policies should also be reviewed and security awareness training included as part the organisation’s schedule. With this, system failures can be limited and the risk of exploitation can be mitigated if these holes are filled when identified and industry standards are adhered to. Furthermore, through practice and diligence, the company’s assets will be protected and the risk to the organisation’s financial health and reputation limited.

Table of Contents

**Scan Results1**

Methodology2

Assessment Environment3

**Findings4**

Risk Assessment5

Recommendations6

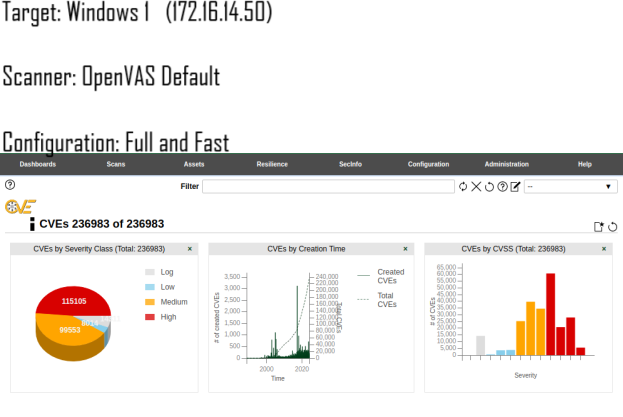
**Summary of Risk Categories7**

Long Term Actions8

References9

Scan Results

**Windows 1**

****

**CVE-2024-30080** – Windows Hyper-V elevation of privilege vulnerability (CVE-2024-30080). An attacker who exploits this vulnerability by accessing a victim guest VM could run arbitrary code in an elevated privilege context (elevated to NT CBTS or NT SYSTEM privilege level) on the victim host system.

Mitigation: Update Hyper-V to the latest update and apply all security patches from Microsoft.

CVSS score base: 9.8

**CVE-2023-36911**: ‘Microsoft Windows Support Diagnostic Tool (MSDT) appeared for remote code execution in security when a user opened a specially crafted document. The attacker can use this vulnerability as to execute arbitrary code within the context of the user who opened this document. It occurs either via phishing emails or malicious websites.

Mitigation: Apply security patches and educate users about the dangers of opening documents from unknown sources.

CVSS base score 9.8

**CVE-2022-34718**: A remote code execution vulnerability in the Windows TCP/IP stack. Arbitrary code execution is possible through the sending of specially crafted packets by an attacker which may lead the system to being compromised.

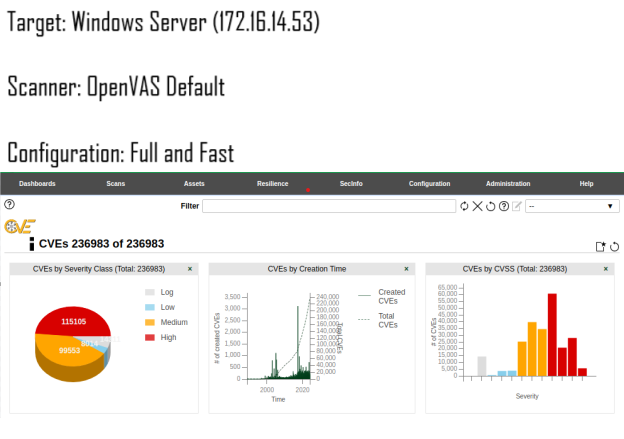
Mitigation: Applying the latest security patches from Microsoft.  
CVSS base score 9.8

**CVE-2022-30190**: Similar in exploitation vector to CVE-2023-36911 from above, a remote code execution in MSDT with the same malicious documents, and same threat for the system integrity and data security since the attacker can execute arbitrary code with the privileges of the user opening the document.

Mitigation: Installation of the latest update from Microsoft and adequate user training on phishing attempts.

CVSS base score 7.8

**Windows Server**

****

**CVE-2024-38077**: Windows Remote Desktop Licensing Service Remote Code Execution (RCE). Unauthenticated remote attackers can cause arbitrary code execution by sending a specially crafted packet to the Remote Desktop Licensing service.

Mitigation: Microsoft has deployed the latest patch.

CVSS base score: 9.8

**CVE-2022-34722**: Remote Code Execution in Windows Internet Key Exchange (IKE) Protocol Extensions; Access Control bypass - HTML; System: This vulnerability could lead to complete system compromise, granting a hacker access and control to the server if left unpatched.

Mitigation: Microsoft's latest security update, along with the updated configurations, would resolve this vulnerability.

CVSS base score: 9.8

**CVE-2024-38104**: An untrusted pointer dereference in the Microsoft Windows Fax Service could allow remote code execution on Windows versions. Successful exploitation of this vulnerability would allow low-privileged attackers to send a crafted request from a remote system that, after successful exploitation, could execute arbitrary code in the context of the targeted system.

Mitigation: Microsoft has released patch updates to prevent exploitation.

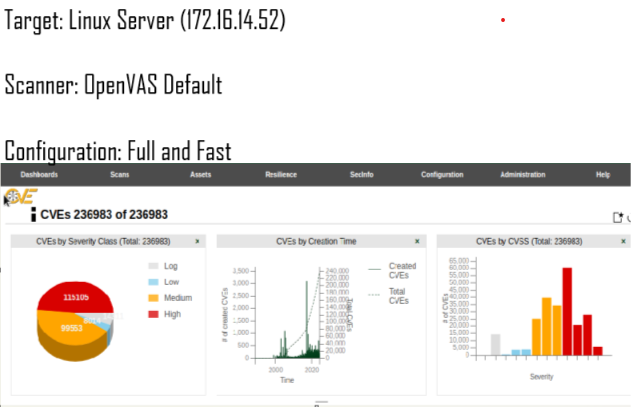
CVSS base score: 8.8

**CVE-2024-38112**: A spoofing vulnerability exists in the Windows MSHTML platform. An attacker can successfully exploit this vulnerability only when an administrator, user or SLAT service is logged on and running Microsoft Edge, Internet Explorer, or Microsoft Office, in some cases. In the worst case, successful exploitation could allow an attacker to execute arbitrary code, run programs, or trick the user into opening a malicious document imported from a malicious site.

Mitigation: The security updates addressed the vulnerability.

CVSS base score: 7.8

**Linux Server**

****

**CVE-2023-32254**: This vulnerability in the Linux kernel contains an in-kernel SMB server named “ksmbd”. It has affected certain Linux distributions with versions 5.10, 5.15, or 5.19. The vulnerability, designated as CVE-2023-32254 in DEB, occurs because SMB uses a robust generic mechanism (RPC/ Ор addressing) that doesn’t perform additional memory synchronisation when handling some commands or credential passing modes. An attacker who exploits this vulnerability can exempt the function from proper synchronisation, leading to concurrent function execution. This subsequently results in a code execution in the kernel memory context, potentially compromising the entire system.

Mitigation: Install patches provided by the Linux kernel maintainers.

CVSS base score: 9.9

**CVE-2023-38432**: Versions before 6.3.10 - ksmbd is a high-performance in-kernel SMB server implemented on top of the NFSv4 protocol stack. The vulnerability is due to the way the kernel's ksmbd rejects an instantiated connection. The relationship between the length of a command payload allocated by the system and the RFC1002 length specification must be validated only through comparison or modulo operations, leading to an out-of-bounds read. This can result into disclosure of sensitive communications, affecting the confidentiality and availability of a target.

Mitigation: Upgrade your Linux kernel.

CVSS base score: 9.1

**CVE-2024-21472**: This vulnerability was related to memory corruption when handling GPU operations. It is a 'use-after-free' type of vulnerability, which means that memory – presumably previously allocated for an object – is freed and then accessed again. Often this will result in a crash of the application or entire system, but it can also lead to arbitrary code execution.

Mitigation: Upatches/updates provided by Qualcomm and apply them as soon as possible.

CVSS base score: 8.4

Methodology

The following vulnerabilities were detected in the networks assessed. Each one is described in terms of its potential impact on a system and includes mitigation suggestions to keep the company's network secure and uncompromised. Base CVSS scores are provided to indicate the potential impact of each vulnerability on the company. During the vulnerability assessment, vulnerabilities were identified and quantified using security tools that conducted in-depth scans of the organization's critical systems. The primary tool used was OpenVAS/GVM (Greenbone Vulnerability Management tool), known for its comprehensive detection capabilities.

This tool was used to conduct scans on:

Windows 1

WinServer

Linux Server

The "Full and Fast Scan" was employed, which quickly identifies common and critical vulnerabilities using a collection of preconfigured plugins with optimal settings. Scans were conducted in a controlled network environment to provide a comprehensive view of the organization's overall security posture and highlight areas of immediate concern.

Assessment Environment

Scans targeted the following systems:

**Windows 1:** Critical for client operations and vulnerable due to user interactions, making it an accessible attack target.

**Winserver:** Essential for server operations and data management.

**Linux server:** Hosts web services and applications, tested to ensure secure configurations and software versions.

By using these tools and scans in a controlled network, we obtained a broad view of the organization's key systems' security posture, identified key vulnerabilities, and provided recommendations to enhance security defenses.

Findings

As stated previously, the vulnerability assessment successfully scanned three critical systems:

Windows 1

Winserver

Linux server.

The scans revealed various vulnerabilities, categorized by severity, including remote code execution and privilege escalation for Windows systems, and critical issues and misconfigurations in Linux server web services and SSH configurations.

The detailed assessments of the organization's security position can form the basis for later risk evaluations and recommendations.

Risk Assessment

This section categorizes all identified vulnerabilities from the vulnerability scans performed on Windows 1, WinServer, and Linux Server. Each vulnerability is listed with details on the affected target/service/software, a description of the issue, recommended solutions, and the number of affected systems. The vulnerabilities are categorized into Critical, High, and Medium severity based on the Common Vulnerability Scoring System (CVSS).

**Critical Vulnerabilities**

**CVE-2024-30080: Elevation of Privilege in Windows Hyper-V**

**Target/Service:** Windows Hyper-V

**Description:** This vulnerability allows an attacker with guest VM access to execute arbitrary code with elevated privileges on the host system, leading to unauthorized actions and access to sensitive data.

**Solution:** Update Hyper-V to the latest version and apply all Microsoft security patches.

**CVSS Base Score:** 9.8

**CVE-2023-36911: Remote Code Execution in Microsoft Windows Support Diagnostic Tool (MSDT)**

**Target/Service:** Microsoft Windows Support Diagnostic Tool (MSDT)

**Description:** This vulnerability allows remote code execution when users open a specially crafted document. An attacker can exploit this to execute arbitrary code within the context of the user opening the document through phishing emails or malicious webpages, potentially leading to data manipulation or unauthorized access.

**Solution:** Apply Microsoft's security patch and educate users on the risks of opening documents from unknown sources.

**CVSS Base Score:** 9.8

**CVE-2022-34718: Remote Code Execution in Windows TCP/IP**

**Target/Service:** Windows TCP/IP stack

**Description:** A vulnerability in the Windows TCP/IP stack that allows an attacker to execute arbitrary code by sending specially crafted packets, compromising the system.

**Solution:** Apply the latest security patches from Microsoft.

**CVSS Base Score:** 9.8

**CVE-2024-38077: Remote Code Execution in Windows Remote Desktop Licensing Service**

**Target/Service:** Windows Remote Desktop Licensing Service

**Description:** This vulnerability allows unauthenticated attackers to execute arbitrary code by sending specially crafted network packets, potentially leading to complete system compromise.

**Solution:** Apply the latest security patch from Microsoft.

**CVSS Base Score:** 9.8

**CVE-2022-34722: Remote Code Execution in Windows Internet Key Exchange (IKE) Protocol Extensions**

**Target/Service:** Windows Internet Key Exchange (IKE) Protocol Extensions

**Description:** This vulnerability allows remote attackers to execute arbitrary code by sending specially crafted IP packets to a target system with IPsec enabled, compromising system security.

**Solution:** Apply the latest security patch from Microsoft and update configurations.

**CVSS Base Score:** 9.8

**CVE-2023-32254: Remote Code Execution in Linux Kernel (ksmbd)**

**Target/Service:** Linux Kernel (ksmbd)

**Description:** A vulnerability in the Linux kernel’s ksmbd component due to improper synchronization when handling specific commands, allowing an attacker to execute code with kernel-level privileges, potentially leading to complete system compromise.

**Solution:** Apply patches from the Linux kernel maintainers and monitor for related advisories.

**CVSS Base Score:** 9.9

**CVE-2023-38432: Out-of-Bounds Read in Linux Kernel (ksmbd)**

**Target/Service:** Linux Kernel (ksmbd)

**Description:** This vulnerability, affecting versions before 6.3.10, involves improper validation leading to an out-of-bounds read, potentially granting unauthorized access to sensitive information.

**Solution:** Update the Linux kernel to the latest version.

**CVSS Base Score:** 9.1

High Vulnerabilities

**CVE-2022-30190: Remote Code Execution in Microsoft Windows Support Diagnostic Tool (MSDT)**

**Target/Service:** Microsoft Windows Support Diagnostic Tool (MSDT)

**Description:** This vulnerability can be exploited via malicious documents, allowing attackers to execute arbitrary code with the privileges of the user who opens the document, posing significant risk to system integrity and data security.

**Solution:** Patch the vulnerability with the latest update from Microsoft and provide user training on recognizing phishing attempts.

**CVSS Base Score:** 7.8

**CVE-2024-38104: Remote Code Execution in Windows Fax Service**

**Target/Service:** Windows Fax Service

**Description:** This vulnerability involves an untrusted pointer dereference in the Windows Fax Service, allowing low-privilege attackers to execute arbitrary code by sending specially crafted requests.

**Solution:** Apply the latest security patches from Microsoft.

**CVSS Base Score:** 8.8

**CVE-2024-38112: Spoofing Vulnerability in Windows MSHTML Platform**

**Target/Service:** Windows MSHTML Platform

**Description:** This vulnerability requires user interaction, such as opening a malicious file, leading to the user believing they are interacting with a legitimate source.

**Solution:** Apply current security patches from Microsoft.

**CVSS Base Score:** 7.8

**CVE-2024-21472: Memory Corruption in Linux Kernel (GPU Operations)**

**Target/Service:** Linux Kernel (GPU Operations)

**Description:** A memory corruption issue during GPU operations, classified as a "use-after-free" flaw, potentially leading to arbitrary code execution, system crashes, or unexpected behaviors.

**Solution:** Apply patches and updates provided by Qualcomm.

**CVSS Base Score:** 8.4

Summary of Risk Categories

**Critical:** Vulnerabilities that can lead to complete system compromise, allowing attackers to execute arbitrary code, gain elevated privileges, or access sensitive data. Immediate action is required.

**High:** Vulnerabilities that pose significant risks to system integrity and data security, potentially leading to unauthorized access, data breaches, or further exploitation. Prompt mitigation is necessary.

**Medium:** Vulnerabilities that can be exploited with lower impact or require more complex attack vectors. Mitigation is essential but less urgent than critical or high vulnerabilities.

**Low:** Minor vulnerabilities that pose minimal risk but should still be addressed to maintain overall security hygiene. Regular updates and maintenance are sufficient.

Recommendations

**1. Hyper-V Update and Security Patching:**

**Rationale:** Elevation of privilege vulnerabilities (CVE-2024-30080) can grant attackers elevated access, jeopardizing system integrity and sensitive data.

**Action:** Upgrade Hyper-V to the latest version and apply all Microsoft-released security patches.

**2. User Training:**

**Rationale:** Remote code execution vulnerabilities in MSDT (CVE-2023-36911, CVE-2022-30190) can be exploited via phishing and malicious documents, potentially compromising user systems.

**Action:** Conduct thorough user training to help users identify phishing attempts and understand the risks of opening documents from unknown sources.

**3. Critical Vulnerabilities Security Patching:**

**Rationale:** Critical vulnerabilities can lead to severe risks, such as remote code execution and system compromise. Prompt addressing of these issues reduces the likelihood of exploitation.

**Action:** Patch Windows Remote Desktop Licensing Service, Windows Internet Key Exchange (IKE) Protocol Extensions, and Linux kernel components according to the guidelines from Microsoft and Linux kernel maintainers.

**4. High Vulnerabilities Security Patching:**

**Rationale:** High-severity vulnerabilities risks like arbitrary code execution and spoofing attacks.

**Action:** Apply the latest security patches for Windows Fax Service, MSHTML platform, and Linux kernel GPU operations.

**5. Windows TCP/IP Stack Update:**

**Rationale:** The medium-severity remote code execution vulnerability in the TCP/IP stack can compromise the system if not patched.

**Action:** Install the latest security patches from Microsoft to mitigate this issue.

**6. Security Configuration Review and Enhancement:**

**Rationale:** Proper configurations prevent exploitation of vulnerabilities and bolster system security.

**Action:** Audit configurations for OpenSSH, web servers, and network services. Enforce strong encryption, minimize unnecessary services, and ensure robust access controls.

Long-term Actions

1. **Regular Security Training and Awareness:**

**Rationale:** Educated employees are less susceptible to phishing and can recognize suspicious activities, lowering the risk of exploitation.

**Action:** Conduct regular training sessions and awareness campaigns on cybersecurity best practices, phishing recognition, and sensitive data handling.

1. **Robust Patch Management Process:**

**Rationale:** Timely updates are crucial to prevent exploitation of known vulnerabilities.

**Action:** Establish a regular patch management schedule and implement automated patch deployment processes to ensure timely updates.

1. **Periodic Security Assessments and Audits:**

**Rationale:** Regular assessments identify new vulnerabilities and misconfigurations, aiding continuous security improvement.

**Action:** Schedule frequent vulnerability assessments, penetration tests, and security audits to identify and address potential weaknesses.

1. **Security Policy Review and Update:**

**Rationale:** Up-to-date security policies provide clear guidelines for maintaining a secure environment.

**Action:** Regularly review and update security policies to align with best practices and compliance requirements, covering access controls, data protection, incident response, and user behavior.

1. **Enhanced Access Controls and Authentication:**

**Rationale:** Strong access controls and authentication mechanisms minimize the risk of unauthorized access and data breaches.

**Action:** Implement multi-factor authentication (MFA), enforce strong password policies, and periodically review user access privileges.

1. **Continuous Monitoring and Incident Response:**

**Rationale:** Continuous monitoring allows early detection of potential security incidents, enabling swift response and mitigation.

**Action:** Deploy advanced monitoring tools for continuous network and system activity tracking. Develop a robust incident response plan for quick and effective handling of security incidents.

By implementing these recommendations, the organization can strengthen its security posture, minimize exploitation risks, and safeguard critical systems and sensitive data. Immediate actions target the most urgent vulnerabilities, while long-term strategies build a foundation for ongoing security enhancement and resilience.

# Thank you.

***Briefing***

<https://github.com/i-Kodoku/Home/blob/1e50ad0dd778d9b68ad975ea64f36a3b28fdb8e6/Cat's%20Company%20Holes%20Revealed%20Briefing%20.pptx>

References

# Greenbone openvas. OpenVAS. <https://www.openvas.org/>

# NVD. <https://nvd.nist.gov/>

# Latest Wampserver Vulnerabilities. <https://feedly.com/cve/vendors/wampserver>

# CVE-2022-36714 The Lab Management System v1.0 had a SQL injection vulnerability in the Section parameter.. <https://www.cve.news/cve-2022-36714/>

# Mitigation Instructions for CVE-2010-2730. <https://cyrisk.com/security/mitigation-instructions-for-cve-2010-2730>

# CVE-2022-30190 (Follina) explained. <https://www.hackthebox.com/blog/cve-2022-30190-follina-explained>

# Bentley View - Security Vulnerabilities in 2024. <https://stack.watch/product/bentley/bentley-view/>

# CVE-2023-38432. <https://security-tracker.debian.org/tracker/CVE-2023-38432>

# CVE-2022-36714 The Lab Management System v1.0 had a SQL injection vulnerability in the Section parameter.. <https://www.cve.news/cve-2022-36714/>

[Sample Network Vulnerability Assessment Report](https://purplesec.us/wp-content/uploads/2019/03/Sample-Network-Security-Vulnerability-Assessment-Report-Purplesec.pdf)from PurpleSec. <https://purplesec.us/wp-content/uploads/2019/03/Sample-Network-Security-Vulnerability-Assessment-Report-Purplesec.pdf>

[Security Assessment Report Template](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/Security-Assessment-Report-Template.docx) (Word format) from CMS.gov. <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/Security-Assessment-Report-Template.docx>

ChatGPT - <https://chatgpt.com/>

GPT for Excel Word - <https://appsource.microsoft.com/en-us/product/office/wa200005502?tab=overview>