



CORVIT Institute
CVE-2024-38063 Assessment Report

Business Confidential

Date: August 8th, 2024

Version: 1.0

Table of Contents

Confidentiality Statement 3

Disclaimer 3

Contact Information 3

Kunlun Lab: Brief Description..... 4

Kunlun Lab Security Researcher: Xiao Wei 4

Assessment Overview..... 4

Technical Details 5

 Key Technical Points 5

How Does CVE-2024-38063 Work? 6

Exploitability 6

 Attack Vector 6

Wormability..... 7

Impact of CVE-2024-38063..... 7

 Scale of Infection 7

 Potential for Ransomware Attacks 7

Mitigations 8

Recommendations 8

Conclusion 9

Confidentiality Statement

This document is the exclusive property of CORVIT Institute. This report contains sensitive and proprietary information intended solely for the recipient's use. Unauthorized disclosure, distribution, or copying of this document is strictly prohibited. The information provided herein is for internal use and should not be shared with external parties without prior written consent. All efforts have been made to ensure the accuracy of the information contained within this report; however, it is the responsibility of the recipient to protect and manage the information in accordance with their organization’s security policies.

Disclaimer

The contents of this report are provided for informational purposes only. While every effort has been made to ensure the accuracy and completeness of the information, the authors and their associated organizations make no representations or warranties, express or implied, regarding the validity or reliability of the data and recommendations provided. The report should not be considered as legal, professional, or security advice, and the reader assumes full responsibility for the application of any actions or decisions based on this information. The authors accept no liability for any direct, indirect, or consequential damages resulting from the use or misuse of this report.

Contact Information

| Name | Contact | Email |
|------------------|-------------|---------------|
| Abdul Moiz | 12345678910 | abc@gmail.com |
| CORVIT Institute | 32145698710 | xyz@gmail.com |

Kunlun Lab: Brief Description

Kunlun Lab is a cybersecurity research company known for its work in vulnerability discovery, exploit development, and offensive security research. Founded by leading security experts, Kunlun Lab focuses on uncovering critical vulnerabilities in widely-used software and systems, such as Windows, Android, and popular cloud platforms. The company's research has been recognized at major cybersecurity conferences, and they are notable for their contributions to the discovery of high-impact vulnerabilities, such as **CVE-2024-38063**, highlighting their expertise in network and system security.

Kunlun Lab Security Researcher: Xiao Wei

Xiao Wei is a security researcher at Kunlun Lab, specializing in vulnerability discovery and exploit development. Known for his expertise in offensive security, Xiao Wei has made significant contributions to the cybersecurity community by identifying critical vulnerabilities in widely-used systems, such as Windows. His research focuses on network protocols and system internals, with a particular emphasis on zero-click exploits. Xiao Wei's work, including the discovery of CVE-2024-38063, has been recognized for its impact on improving global security practices.

Assessment Overview

CVE-2024-38063 is a critical vulnerability affecting all Windows systems that have IPv6 enabled by default. This vulnerability stems from an integer underflow flaw in the Windows TCP/IP stack, which can be exploited remotely to achieve Remote Code Execution (RCE) without user interaction. It poses a high risk due to its zero-click nature, making it particularly dangerous and wormable.

| | |
|-------------------|--|
| CVE ID: | CVE-2024-38063 |
| Discovered By: | Kunlun Lab’s security researcher, Xiao Wei |
| Severity: | Critical |
| CVSS Score: | 9.8 |
| Affected Systems: | All Windows systems with IPv6 enabled, including Windows 10, Windows 11, and Windows Server. |

Technical Details

The root of CVE-2024-38063 lies in the Windows TCP/IP stack, specifically in how it handles IPv6 packets. The flaw is caused by an **integer underflow**, which can lead to **buffer overflows**. When an attacker sends a specially crafted IPv6 packet to a vulnerable system, this overflow can result in the execution of malicious code. This vulnerability can be exploited remotely, meaning an attacker does not need physical access to the target machine. Once exploited, the attacker could gain the same level of access and control as the current user, leading to potential system compromise.

Exploitable Conditions: The vulnerability requires that IPv6 be enabled on the affected system. If IPv6 is not in use, the risk from this particular vulnerability is mitigated.

Attack Vector: Exploitation can occur over the network. An attacker sends specially crafted IPv6 packets to the target system, triggering the vulnerability.

Impact: If successfully exploited, the attacker can execute arbitrary code on the target machine. This could lead to a complete system compromise if the attacker escalates privileges or performs other malicious activities.

Key Technical Points

| | |
|------------------------|--|
| Type of Vulnerability: | Integer Underflow leading to Buffer Overflow. |
| Affected Protocol: | IPv6 within the TCP/IP stack. |
| Attack Vector: | Remote, requiring no user interaction. |
| Exploit Complexity: | Low. It can be triggered by sending a malformed IPv6 packet repeatedly. |
| Impact: | Complete compromise of the target system, including potential for arbitrary code execution and privilege escalation. |

How Does CVE-2024-38063 Work?

The core issue with CVE-2024-38063 lies in the way Windows handles IPv6 packets. When IPv6 is enabled, the operating system must process and manage network traffic that uses this protocol. The vulnerability in question arises due to insufficient validation of certain packets, which could allow an attacker to send specially crafted network requests that the system fails to properly handle.

- 1. Exploit Initiation:** An attacker sends malicious IPv6 packets to a target Windows system.
- 2. Vulnerability Trigger:** Due to improper handling of these packets, the system's response may result in execution of arbitrary code.
- 3. Remote Execution:** The attacker gains control over the affected system, potentially compromising sensitive data or performing unauthorized actions.

Exploitability

The exploitability of CVE-2024-38063 lies in its combination of zero-click nature and network-based attack vector. Here's a deeper look into the exploitability aspects:

Attack Vector

- **Remote Exploit**

This vulnerability can be exploited remotely, meaning an attacker does not need physical access to the target system. The attacker can be anywhere on the network, including across the internet, provided they have network access to the vulnerable machine's IPv6 interface.

- **Zero-Click**

No user interaction is required for exploitation. Unlike phishing attacks or social engineering, the vulnerability does not rely on tricking the user into clicking a link or downloading a file. The mere receipt of a specially crafted IPv6 packet is enough to trigger the flaw, making this vulnerability particularly dangerous and stealthy.

Wormability

One of the most concerning aspects of CVE-2024-38063 is its **wormable nature**. Wormable vulnerabilities can be exploited to propagate automatically from one system to another, often leading to widespread outbreaks. If attackers craft a worm leveraging this vulnerability, it could cause significant damage across corporate and home networks.

Wormable Nature: A wormable vulnerability allows attackers to exploit a flaw in one system and then use that compromised system to automatically attack other vulnerable systems. In this case, the attacker would send a specially crafted IPv6 packet to the target machine, triggering the vulnerability. Once the vulnerability is exploited and the attacker gains control of the system, they can use that machine to launch further attacks on other connected systems, creating a self-replicating "worm" effect.

Impact of CVE-2024-38063

The implications of CVE-2024-38063 are severe. Since it allows RCE, an attacker could potentially gain full control over the compromised system. This could lead to:

- Unauthorized access to sensitive information.
- Disruption of system operations.
- Installation of additional malicious software or malware.

Given that the vulnerability affects all versions of Windows with IPv6 enabled, the scope of potential impact is broad, affecting both individual users and large organizations.

Scale of Infection

In corporate networks where thousands of machines may be connected, a worm leveraging this vulnerability could infect a large portion of the network within minutes. This would result in widespread disruption, potentially taking down critical services, disrupting business operations, and causing financial and reputational damage.

Potential for Ransomware Attacks

Once the vulnerability is exploited and control of a system is gained, attackers can deploy various payloads, such as ransomware. This could result in large-scale ransomware campaigns, where entire networks are encrypted, and businesses are forced to pay ransoms to regain access to their data.

Mitigations

Microsoft has released a patch as part of their August 2024 Patch Tuesday update. Users are strongly advised to apply these updates as soon as possible to mitigate the risks associated with this vulnerability.

Mitigation Strategies

1) Disable IPv6

Although not recommended long-term, disabling IPv6 can temporarily reduce the attack surface for this vulnerability. However, Microsoft warns that this may impact other Windows functionalities, as IPv6 is a core component of modern Windows systems.

2) Firewall Configurations

Employing network-based mitigations, such as configuring firewalls to block unwanted IPv6 traffic, could help reduce exposure.

3) Monitor and Respond

Implement monitoring solutions to detect unusual or unauthorized IPv6 traffic. An effective monitoring system can help identify and respond to potential exploits.

4) Update Systems

Ensure that your Windows systems are up-to-date with the latest security updates and patches. Keeping systems current can help protect against known vulnerabilities.

Recommendations

1) Apply Patches Immediately

Administrators and users should prioritize installing the August 2024 security update.

2) Network Defense-in-Depth

Beyond patching, consider enhancing network monitoring, implementing IDS, and ensuring robust firewall configurations to detect and block malicious IPv6 traffic.

3) Evaluate IPv6 Usage

Assess the necessity of IPv6 in your environment. If it is not required, consider temporarily disabling it while testing for the impact of patches.

Conclusion

CVE-2024-38063 represents a significant threat to the security of Windows systems worldwide. Its zero-click, wormable nature makes it especially dangerous, and organizations must take immediate steps to secure their environments. By applying the appropriate patches and considering additional mitigations, users can significantly reduce the risk of exploitation.

For detailed patch instructions, users should refer to Microsoft's security update documentation and follow any additional best practices recommended by their network security teams.