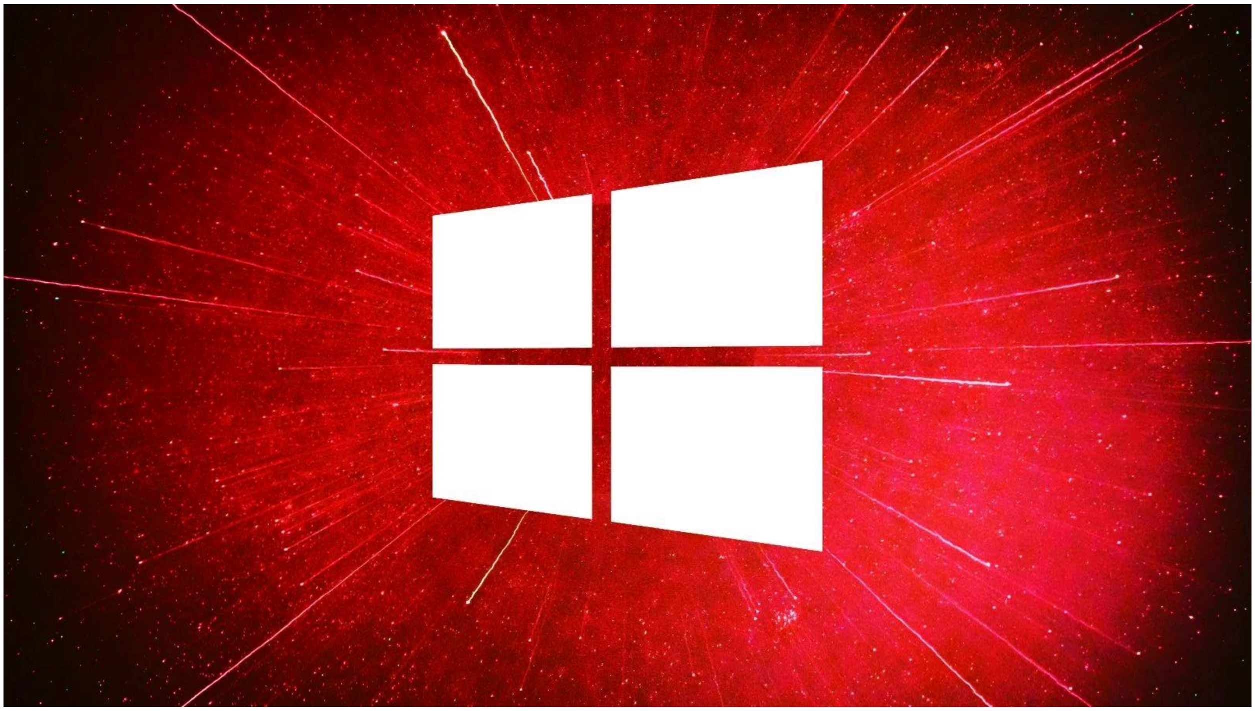
Serianu Advisory on Windows TCP/IP RCE Vulnerability CVE-2024-38063



Threat Scenario:

Microsoft disclosed a **critical** (**CVSS** 9.8) TCP/IP Remote Code Execution (RCE) vulnerability that affects and impacts all Windows systems utilizing IPv6.

CVE-2024-38069 is a Remote Code Execution vulnerability that affects all versions of Windows systems that have IPv6 enabled. The flaw allows an attacker to execute arbitrary code on a target machine from a remote location, making it a sever security flaw. The vulnerability arises from how the Windows TCP/IP stack process IPv6 packets, that could create a pathway for an attacker to compromise the system. Once exploited the attacker could gain the same level of access and control as the current user. This is a Zero-click vulnerability which means it does not need user interaction to be exploited, the attacker can exploit the vulnerability from a remote location.

Threat Target:

- **Windows Systems** – The vulnerability affects all versions of Windows, including Windows 10, Windows 11 and Windows Server editions (2016, 2019 and 2022)
- **Critical Infrastructure** – All sensitive entities/systems handling IPv6 packets are at risk. These include corporate networks, financial institutions and government agencies who are primary targets due to the high impact on confidentiality, integrity and availability.
- **Insider Threat** – The attack requires local access, even those with low privileges. No user interaction is needed, making it more accessible for an insider threat or a compromised system within an organization.

Threat Actor:

- **Insider Threats:** Individuals within an organization with the knowledge of this vulnerability and knowledge of the organization's deployed protocols with local access could leverage this vulnerability to conduct malicious activities.
- **Cybercriminals and organized Threat actor groups:** These groups could potentially deploy automatic scanners for detection of this vulnerability and gain unauthorized access to systems where they could steal sensitive information or deploy ransomware.
- **Advanced Persistent Threats (APTs):** APT groups, known for their stealthy and prolonged existence in local networks can leverage this vulnerability infiltrate networks, escalate privileges and further advance their covert capabilities for espionage and sabotage purposes.
- **Nation-State Actors:** Governments or state-sponsored groups may exploit this vulnerability to target high-value systems particularly those in critical infrastructure, government or defense sectors.

Threat Indicators:

- **Unusual IPv6 Activity:** Anomalous IPv6 behavior on the network could indicate a potential exploit of the vulnerability.
- **Unusual Certificate Activity:** Unexpected changes in system or application certificates. Invalid or untrusted certificates being used in cryptographic operations.
- **EDR and SIEM Monitoring Alerts:** Alerts for Endpoint Detection and Response (EDR) solutions or Security Information and Event Management (SIEM) highlighting security events related to certificate changes or IPv6 anomalous behavior.
- **Detection by Vulnerability Scanners:** Detecting and blocking vulnerability scanners. This indicator suggests that an attacker may be attempting to exploit the vulnerability or already succeeded in doing so.

Risk Scenario(s):

- **Supply Chain Attacks:** If a trusted vendor's system is compromised using this vulnerability, an attacker could introduce malicious code into software or network spreading compromise and leverage into downstream users or systems.
- **National Security Risks:** Could lead to disruption of critical infrastructure e.g Energy grids, water supply, Health services or theft of classified information.
- **Compromise of Encrypted Communications:** The vulnerability could be used to intercept or alter encrypted communications within a network, especially in environments where secure communication channels are critical like financial institutions and government agencies. This could lead to man-in-the-middle attacks, where attackers could eavesdrop, steal data or insert malicious content into legitimate communications.
- **Unauthorized access to Sensitive Data:** Exploiting this vulnerability could allow an attacker to access encrypted files by bypassing cryptographic protections. This would have a high impact of sensitive information including personal data, corporate secrets or government data leading to severe confidentiality breaches.
- **Legal action:** By compromising confidentiality breaches and other compliance requirements organizations may face fines, legal actions and damage to their reputation.

Risk Exposure: Data confidentiality, System Integrity, Disruption to Business Continuity, Supply Chain and Third-party risks, Regulatory Compliance (Failure to compliance regulations like GDPR or HIPAA)

Recommended Threat Mitigation Actions:

- **Implement Patch released on August 13, 2024:** Ensure Windows systems are up to date with the latest security updates and patches.
- **Prioritize patching Internet Facing devices**
- **Disable IPv6 if IPv6 is not required**
- **Monitor and Respond:** Monitor for any suspicious activity, particularly involving IPv6 traffic.
- **Implement Network Segmentation:** to limit potential lateral movement if a system is compromised.
- **Least Privileged Principle:** Limiting user privileges can reduce the risk of exploitation by restricting access to critical functions that could be leveraged by the attacker.

Conclusion

CVE-2024-38069 presents a critical risk to all Windows systems with IPv6 enabled, underscoring the importance of maintaining up-to-date security practices. By understanding the nature of this vulnerability and implementing the appropriate measures, organizations can better safeguard their systems and mitigate the risks associated with such emerging threats.

It is critical you perform an analysis of your environment, validate that these controls have been implemented and that you have visibility on all local and vendor IPv6 activities and changes being made to critical systems by your internal team. This will require the collective cooperation of IT, Risk and Audit.

We encourage recipients who are unsure of their security posture, unsure of their technical capabilities to implement the above recommendations and/or identify malicious activity or use of tools or techniques that seem malicious to contact us on the following:

Helpdesk +254(0)716137017, Cybercrime hotline +254 771949475, email: Info@serianu.com.