Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Windows Update Zero-Day Flaws Allow Downgrade Attacks on Patched Systems

Date of Publication	Admiralty Code	TA Number
August 9, 2024	A2	TA2024307

Summary

First Seen: February 2024
Affected Product: Microsoft Windows
Impact: Two recently discovered zero-day vulnerabilities in Windows, CVE-2024-38202 and CVE-2024-21302, enable attackers to downgrade systems, removing security updates and exposing them to old exploits. This attack is undetectable, as Windows Update falsely indicates the system is fully patched. Microsoft is working on mitigations, but no fix is available yet, leaving systems at risk.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38202	Windows Update Stack Elevation of Privilege Vulnerability	Microsoft Windows	✓	☒	☒
CVE-2024-21302	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	Microsoft Windows	✓	☒	☒

Vulnerability Details

#1

A recently discovered two zero-day vulnerabilities in Windows operating systems poses a significant threat to users. These vulnerabilities named, CVE-2024-38202 and CVE-2024-21302, that allow attackers to downgrade Windows systems. This "unpatches" the system, effectively removing installed security updates and making it vulnerable to previously patched exploits. The attack is particularly concerning because it bypasses detection, leaving the Windows Update interface falsely indicating that the system is fully patched.

#2

The vulnerabilities enable attackers to disable Windows virtualization-based security (VBS) features like Credential Guard and Hypervisor-Protected Code Integrity (HVCI), even when enforced with UEFI locks. Attackers with basic user privileges can exploit CVE-2024-38202 to "unpatch" previously mitigated security bugs, while CVE-2024-21302 allows admin-level attackers to replace Windows system files with outdated versions. This exploit highlights a significant flaw in the Windows Update process, which fails to protect against rollback attacks.

#3

Microsoft has acknowledged the issue and is working on mitigation strategies. However, a comprehensive fix has not yet been released. Users and administrators are advised to stay vigilant and monitor for any unusual system behavior, particularly related to Windows Update statuses. Until a fix is available, systems remain at risk, and the potential for widespread exploitation is significant.

#4

The attack is undetectable by endpoint detection and response (EDR) solutions, as Windows Update still reports the system as fully updated despite being downgraded. The potential consequences of this vulnerabilities are severe, as it could allow attackers to gain control over compromised systems. It's crucial for users and organizations to stay informed about the situation and take necessary precautions to protect their systems.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38202	Windows: 10 - 11 23H2 Windows Server: 2016 – 2022 23H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-284
CVE-2024-21302	Windows: 10 - 11 23H2 Windows Server: 2016 – 2022 23H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-284

Recommendations

Disable Automatic Updates Temporarily: Until a patch is released, disabling automatic updates can prevent potential rollback exploits.

Monitor for Update Irregularities: Regularly check the status of installed updates and investigate any unexpected rollbacks.

Regularly Monitor and Audit Systems: Conduct regular audits of your Windows systems to ensure they are running the latest updates and patches. Use logging tools to monitor for unusual activities related to Windows Update processes.

Implement Strong Access Controls: Limit user privileges to reduce the risk of unauthorized access. Regular users should not have administrative rights unless absolutely necessary. Implement role-based access control (RBAC) RBAC to ensure that only authorized personnel can perform updates or modifications to critical systems.

Use Endpoint Detection Tools: Employ advanced security tools that can detect and respond to unusual system behavior.

Segregate Networks: Network segmentation can help isolate vulnerable systems and prevent lateral movement if an attacker gains access. This practice is essential for maintaining the integrity of critical systems and data.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0005 Defense Evasion	TA0004 Privilege Escalation	T1588.005 Exploits
T1068 Exploitation for Privilege Escalation	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1553 Subvert Trust Controls
T1222 File and Directory Permissions Modification	T1203 Exploitation for Client Execution		

Patch Details

Microsoft is working on a patch to fix vulnerabilities CVE-2024-38202 and CVE-2024-21302, but it has yet to be released.

References

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202

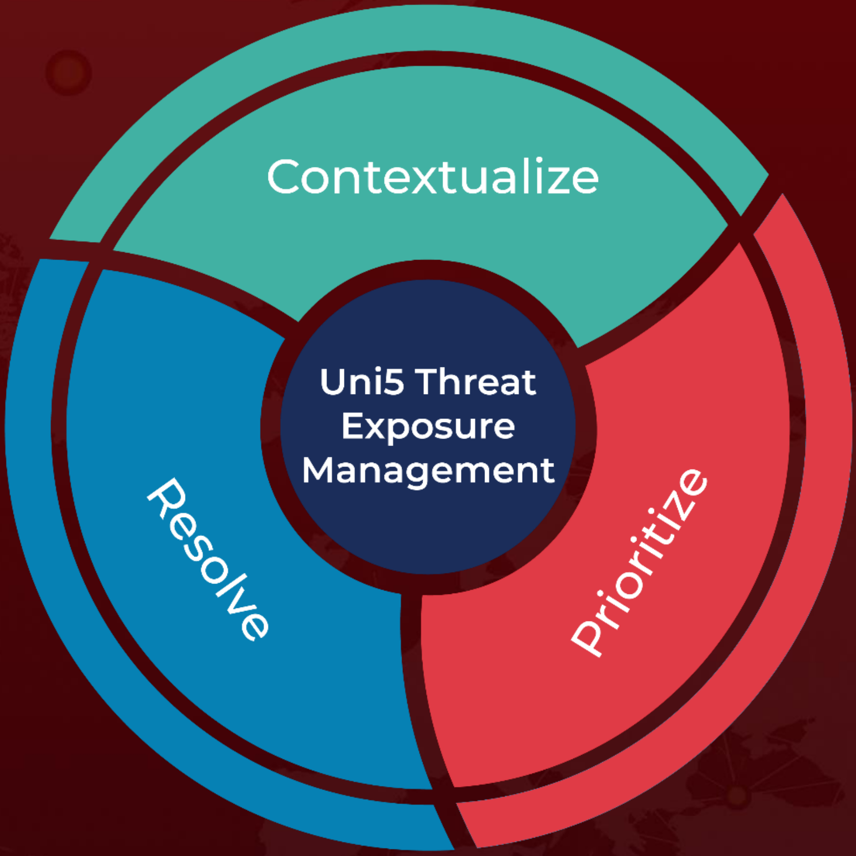
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302

https://www.safebreach.com/blog/downgrade-attacks-using-windows-updates/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 9, 2024 • 5:30 AM

More at www.hivepro.com