KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft patches Windows zero-day DogWalk

Tracker ID: TN0819 **Date:** 16/Aug/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Microsoft has published security fixes to address a high-severity Windows zero-day vulnerability whose exploit is publicly available and being utilized in attacks. The recently patched security bug is tracked as CVE-2022-34713 and goes by the name "DogWalk." All supported Windows versions, including the most recent client and server releases, Windows 11 and Windows Server 2022, are impacted by DogWalk and are being actively exploited.

Attackers can get remote code execution on compromised systems by exploiting this path traversal vulnerability in the Windows Support Diagnostic Tool (MSDT). Attackers can leverage the DogWalk vulnerability to add deliberately generated executables to the Windows Startup when the target downloads the maliciously crafted .diagcab file, which could be shared through email or downloaded from the internet. Consequently, it allows the threat actor to run the planted executables automatically when the victims restart their Windows devices to complete various activities, such as downloading other malware payloads.

Although unauthenticated attackers can exploit the vulnerability in low-complexity attacks, successful exploitation requires user input, such as persuading the victim into opening malicious email attachments or clicking a link to download and launch the malicious file. An attacker could use the flaw in a phishing attempt by sending the target an email with a specially created file and enticing them to open it. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability.

Last month, Microsoft released an official security update for the actively exploited Windows MSDT zero-day known as Follina. Microsoft has also resolved CVE-2022-30134, a Microsoft Exchange Information Disclosure Vulnerability that allows attackers to view targeted email messages. Microsoft addressed 112 vulnerabilities in total as part of the August 2022 Patch Tuesday, including 17 critical ones that allowed privilege escalation and remote code execution.

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-34713	High	7.8
CVE-2022-30134	Medium	5.3

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft patches Windows zero-day DogWalk

Tracker ID: TN0819 **Date:** 16/Aug/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Affected Products and Versions

Windows Server 2012 and 2012 R2 (Server Core installation)

Windows Server 2012 and 2012 (Server Core installation)

Windows Server 2008 R2 for x64-based Systems Service Pack 1 and Server Core installation

Windows RT 8.1

Windows 8.1 for x64-based and 32-bit systems

Windows 7 for x64-based and 32-bit Systems Service Pack 1

Windows Server 2016 and 2016 (Server Core installation)

Windows 10 Version 1607 for x64 and 32-bit based Systems

Windows 10 for x64-based and 32-bit Systems

Windows 10 Version 21H2 for x64-based Systems, ARM64-based Systems and 32-bit Systems

Windows 11 for ARM64 and x64-based Systems

Windows Server, version 20H2 (Server Core Installation)

Windows 10 Version 20H2 for ARM64 , 32-bit and x64-based Systems

Windows Server 2022 and 2022 (Server Core installation)

Windows Server Windows 10 Version 21H1 for 32-bit , ARM64 and x64-based Systems

Windows Server 2019 and 2019 (Server Core installation)

Windows 10 Version 1809 for ARM64, x64 and 32-bit based Systems

Recommendations

- Immediately identify the vulnerable instances and apply the vendor-provided fixes as soon as possible.
- Collect and review relevant logs, data, and artifacts to ensure the threat is eradicated from the network and thwart residual issues that could enable follow-on exploitation.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Microsoft patches Windows zero-day DogWalk

Tracker ID: TN0819 **Date:** 16/Aug/2022 **Category:** Vulnerability **Industry:** All **Region**: All

References

- Sergiu Gatlan, Microsoft patches Windows DogWalk zero-day exploited in attacks, Bleeping Computer, 09th August 2022, External Link (bleepingcomputer.com)
- Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability, Microsoft, 09th August 2022, External Link (msrc.microsoft.com)
- CVE-2022-34713 Detail, NIST, 09th August 2022, External Link (nvd.nist.gov)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471