Hive Pro

Threat Level

Amber

THREAT ADVISORY

VULNERABILITY REPORT

Zero-day vulnerability in Windows terminal management tool gets a hotfix

Date of Publication	Admiralty code	TA Number
September 22, 2022	A1	TA2022210

Summary

Microsoft Endpoint Configuration Manager (MECM) has a spoofing vulnerability that allows remote attackers to access sensitive data. The zero-day vulnerability has been identified as CVE-2022-37972.

CVE Table

CVE	NAME	PATCH
CVE-2022-37972	Microsoft Endpoint Configuration Manager Spoofing Vulnerability	✓

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**T1190** Exploit Public-Facing Application	**TA0006** Credential Access	**T1555** Credentials from Password Stores
T1555.004 Windows Credential Manager	**T1557** Adversary-in-the-Middle		

Technical Details

#1 This vulnerability affects Microsoft Endpoint Configuration Manager (MECM), a management application for Windows terminals including endpoints and servers.

#2 While the "Microsoft Endpoint Configuration Manager" option settings disable the use of "NTLM" as an alternative authentication method, "NTLM" will be used if an authentication error occurs in "Kerberos," which caused CVE-2022-37972.

#3 Currently, no exploitation has been reported. The vulnerability has already been publicly disclosed, but the exploitability index is "Exploitation Less Likely", which is the second-lowest level.

#4 An out-of-the-box update has been released by Microsoft to address this vulnerability. It is recommended to keep "NTLM authentication" disabled as much as possible by default.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-37972	Microsoft Endpoint Configuration Manager: 2103 - 2203	cpe:2.3:a:microsoft:microsoft_endpoint_configuration_manager:*:*:*:*:*:*:*:*	CWE-290

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37972

Reference

https://www.security-next.com/139926

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 22, 2022 . 4:00 AM

More at www.hivepro.com