MANDIANT ADVANTAGE

Vulnerability Report

Microsoft Windows Server 2022 Internet Control Message Protocol (ICMP) Unspecified Vulnerability

Vulnerability (VU)

March 14, 2023 05:45:24 PM, 23-00004484, Version: 1

Risk Rating: HIGH | Exploitation State: No Known

Executive Summary

An unspecified vulnerability exists within the Internet Control Message Protocol (ICMP) component in Microsoft Windows Server 2022 and earlier that, when exploited, allows a remote attacker to execute arbitrary code. Exploit code is not publicly available. Mitigation options include a vendor fix.

Description

A remote code execution vulnerability exists in Windows Internet Control Message Protocol (ICMP).
An attacker who successfully exploited the vulnerability could run arbitrary code on the affected system.

Date of Disclosure

March 14, 2023 04:00:00 AM

Threat Detail

An attacker could exploit this vulnerability to execute arbitrary code. The attacker would need to send a low-level protocol error containing a fragmented IP packet inside another ICMP packet in its header to the target machine. To trigger the vulnerable code path, an application on the target must be bound to a raw socket.

Mandiant Threat Intelligence considers this a High-risk vulnerability due to the possibility of remote code execution offset with no user interaction required.

Please rate this product by taking a short four question survey

Vulnerable Products

Microsoft reports that the following products and versions are vulnerable:

- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for x64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 11 version 21H2 for ARM64-based Systems

- Windows 11 version 21H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

First Version Publish Date

March 14, 2023 05:45:24 PM

Exploitation

In the wild	false
Zero Day	false

Technical Tags

Attacking Ease	Easy
Exploitation Vectors	• General Network Connectivity
Exploitation Consequence	Code Execution
Exploitation State	No Known
Mitigation	• Patch
Vulnerability Type	Unknown

Common Vulnerabilities (CVSS V2)

CVSSBaseScore:	10
CVSSTemporalScore:	7.4
Access Vector	AV:N
Access Complexity	AC:L
Authentication	Au:N
Confidentiality Impact	C:C
Integrity Impact	I:C
Availability Impact	A:C
Exploitability	E:U
Remediation	RL:OF
Report Confidence	RC:C

Sources

Title:	Microsoft Corp.
Source URL:	hxxps://msrc[.]microsoft[.]com/update-guide/en-US/vulnerability/CVE-2023-23415
Date:	March 14, 2023 07:00:00 AM
Description:	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability (CVE-2023-23415)

Version Information

Version:1, March 14, 2023 05:45:24 PM

Technology

Vendor - Technology	CPE
microsoft - windows_10 *	cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:x64:*
microsoft - windows_10 *	cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:x86:*
microsoft - windows_10 1607	cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:x64:*
microsoft - windows_10 1607	cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:x86:*
microsoft - windows_10 1809	cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*
microsoft - windows_10 1809	cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:x64:*
microsoft - windows_10 1809	cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:arm64:*:*
microsoft - windows_10 2004	cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:x64:*
microsoft - windows_10 20h2	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:arm64:*
microsoft - windows_10 20h2	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:x86_64:*
microsoft - windows_10 21h2	cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:32-bit:*
microsoft - windows_10 21h2	cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:arm64:*
microsoft - windows_10 21h2	cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:x64:*
microsoft - windows_10 22h2	cpe:2.3:o:microsoft:windows_10:22h2:*:*:*:*:*:32-bit:*
microsoft - windows_10 22h2	cpe:2.3:o:microsoft:windows_10:22h2:*:*:*:*:*:arm64:*
microsoft - windows_10 22h2	cpe:2.3:o:microsoft:windows_10:22h2:*:*:*:*:*:x64:*
microsoft - windows_11 21h2	cpe:2.3:o:microsoft:windows_11:21h2:*:*:*:*:*:arm64:*
microsoft - windows_11 21h2	cpe:2.3:o:microsoft:windows_11:21h2:*:*:*:*:*:x64:*
microsoft - windows_11 22h2	cpe:2.3:o:microsoft:windows_11:22h2:*:*:*:*:*:arm64:*
microsoft - windows_11 22h2	cpe:2.3:o:microsoft:windows_11:22h2:*:*:*:*:*:x64:*
microsoft - windows_server_2008 -	cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*
microsoft - windows_server_2008 r2	cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:x64:*:*:*:*:*
microsoft - windows_server_2008 sp2	cpe:2.3:o:microsoft:windows_server_2008:sp2:*:x64:*:*:*:*:*
microsoft - windows_server_2012 -	cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*
microsoft - windows_server_2012 r2	cpe:2.3:o:microsoft:windows_server_2012:r2:-:-:*:standard:*:*:*
microsoft - windows_server_2016 -	cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:*:*

microsoft - windows_server_2019 *	cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*
microsoft - windows_server_2022 *	cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:*

Common Vulnerabilities and Exposures

CVE ID:	CVE-2023-23415(CVE Description)Mandiant Vulnerability Analysis

MANDIANT ADVANTAGE