

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

Microsoft Addresses Zero-Day and Wormable Vulnerabilities

Date of Publication

April 12, 2023

Admiralty Code

A1

TA Number

TA2023181

Summary










First Seen: April 11, 2023

Affected Product: Microsoft Windows, Windows Server, and Microsoft Raw Image Extension

Impact: Remote Code Execution and Privilege Escalation

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-28252	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows & Windows Server			
CVE-2023-28219	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	Windows & Windows Server			
CVE-2023-28220	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	Windows & Windows Server			
CVE-2023-28232	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	Windows & Windows Server			
CVE-2023-28291	Raw Image Extension Remote Code Execution Vulnerability	Microsoft Raw Image Extension			
CVE-2023-21554	Microsoft Message Queuing Remote Code Execution Vulnerability	Microsoft Message Queuing			
CVE-2013-3900	WinVerifyTrust Signature Validation Vulnerability	WinVerifyTrust function			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-28231	DHCP Server Service Remote Code Execution Vulnerability	Microsoft DHCP Server Service			
CVE-2023-28250	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	Windows Pragmatic General Multicast (PGM)			
CVE-2023-28246	Windows Registry Elevation of Privilege Vulnerability	Microsoft Windows Registry			

Vulnerability Details

#1

In April 2023, Microsoft released Patch Tuesday and security patches to address an actively exploited zero-day vulnerability and 97 other vulnerabilities, which include 7 critical and 90 important flaws. The zero-day vulnerability, identified as CVE-2023-28252, is an elevation-of-privilege flaw in the Windows Common Log File System (CLFS) that affects Windows 10 and Windows Server. Attackers with access to the platform can exploit the vulnerability to gain highly privileged system-level access. Nokoyawa ransomware attacks have been using this Zero-Day vulnerability on systems belonging to small and mid-sized organizations in North America, the Middle East, and Asia.

#2

One crucial patch in Microsoft's April update is CVE-2013-3900, a 10-year-old vulnerability in the Windows WinVerifyTrust function for signature validation. The Lazarus Group from North Korea could have exploited this flaw in a supply-chain attack on 3CX. The attack resulted in malware infecting the company's video-conferencing software systems. When Microsoft released the patch in 2013, it was an opt-in patch due to the potential for the fix to cause problems for some organizations. However, the latest security update in April includes the fix for more platforms.

#3

Microsoft has also patched two critical vulnerabilities in the Layer 2 Tunneling Protocol, tracked CVE-2023-28219 and CVE-2023-28220. In case an unauthenticated attacker sends a connection request to a RAS server, it may lead to remote code execution on the RAS server machine. These vulnerabilities don't require any user interaction, but the adversary has to win a race condition to be successful.

#4

Among the severe issues addressed by Microsoft's April Patch Tuesday update, CVE-2023-21554 stands out as a remote code execution vulnerability in the Microsoft Message Queuing system. An attacker can exploit this vulnerability by sending a specially crafted malicious MSMQ packet, triggering an out-of-bounds write, and executing arbitrary code on the target system. Another vulnerability with a high likelihood of exploitation is CVE-2023-28231, a remote code execution vulnerability in the DHCP server service. To exploit this vulnerability, an attacker would need to gain access to the restricted network and send a specially crafted RCP call to the targeted DHCP server.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-28252	Windows: 10 - 11 22H2 & Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-119
CVE-2023-28219	Windows: 10 - 11 22H2 & Windows Server: 2008 – 2022	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-362
CVE-2023-28220	Windows: 10 - 11 22H2 & Windows Server: 2008 – 2022	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-362
CVE-2023-28232	Windows: 10 - 11 22H2 & Windows Server: 2008 – 2022	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-20
CVE-2023-28291	Raw Image Extension: All versions	cpe:2.3:a:microsoft:raw_image_extension:*:*:*:*:* .*	CWE-20
CVE-2023-21554	Windows: 10 - 11 22H2 & Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-787

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2013-3900	Windows: 7 – XP & Windows Server: 2003 – 2012	cpe:2.3:o:microsoft:windows:-:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*	CWE-310
CVE-2023-28231	Windows Server: 2008 - 2022	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*	CWE-20
CVE-2023-28250	Windows: 10 - 11 22H2 & Windows Server: 2008 – 2022	cpe:2.3:o:microsoft:windows:-:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*	CWE-20
CVE-2023-28246	Windows Server: 2019 – 2022 & Windows: 10 - 11 22H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*	CWE-264

Recommendations



To determine if you are being targeted by the remote code execution vulnerability (CVE-2023-21554) in the Microsoft Message Queuing system, you could verify if a service named "Message Queuing" is running on your machine and if TCP port 1801 is open and listening.



If you are currently using Microsoft Exchange 2013, it is recommended to update to Exchange 2019 or a newer version to obtain the maximum benefits since Exchange 2013 reached its End-of-Life status on April 4, 2023. Additionally, Exchange 2016 will reach its End-of-Life status in October 2025.



Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Potential **MITRE ATT&CK** TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0004</u> Privilege Escalation
<u>TA0005</u> Defense Evasion	<u>TA0040</u> Impact	<u>TA0043</u> Reconnaissance	<u>T1556</u> Modify Authentication Process
<u>T1203</u> Exploitation for Client Execution	<u>T1036</u> Masquerading	<u>T1082</u> System Information Discovery	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1210</u> Exploitation of Remote Services	<u>T1592</u> Gather Victim Host Information	<u>T1190</u> Exploit Public-Facing Application	<u>T1499</u> Endpoint Denial of Service

Patch Links

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28219>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28220>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28232>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28291>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21554>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28231>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28250>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28246>

References

<https://msrc.microsoft.com/update-guide/releaseNote/2023-Apr>

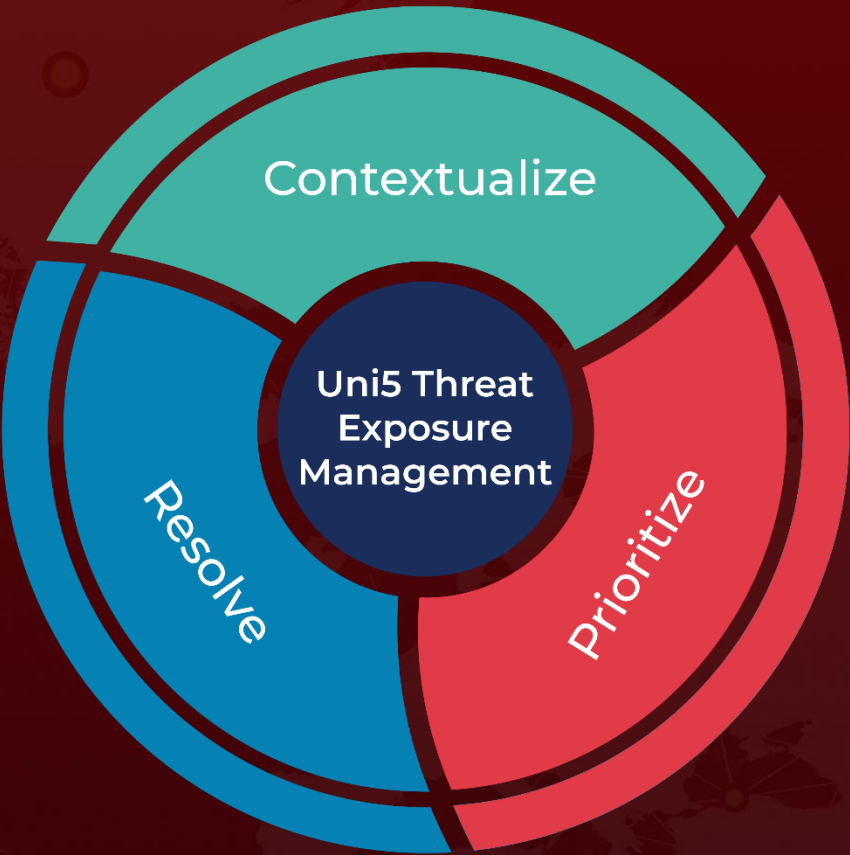
<https://www.hivepro.com/cybercrime-group-exploits-zero-day-on-windows-servers-to-deploy-nokoyawa-ransomware/>

<https://www.darkreading.com/attacks-breaches/3cx-breach-cyberattackers-second-stage-backdoor>

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
April 12, 2023 • 8:38 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com