Hive Pro

THREAT ADVISORY

Microsoft Patch Tuesday fixes critical zero-days along with 97 other flaws	TA2022006
Threat Level RED	**Publish Date –** Jan 12, 2022

Microsoft has fixed 97 vulnerabilities, with nine classified as Critical and 88 as Important and among them 6 zero-days.
Following are the type of security vulnerabilities reported in multiple Microsoft products:
41 Elevation of Privilege Vulnerabilities
29 Remote Code Execution Vulnerabilities
9 Security Feature Bypass Vulnerabilities
6 Information Disclosure Vulnerabilities
9 Denial of Service Vulnerabilities
3 Spoofing Vulnerabilities

Six zero-day vulnerabilities were addressed in the January's patch Tuesday:

- CVE-2021-22947: Remote Code-Execution vulnerability in open-source Curl library.
- CVE-2021-36976: Remote Code-Execution vulnerability in open-source Libarchive.
- CVE-2022-21874: Remote Code-Execution vulnerability in Local Windows Security Center API.
- CVE-2022-21919: Privilege escalation vulnerability in Windows User Profile Service.
- CVE-2022-21839: Denial-of-Service vulnerability in Windows Event Tracing Discretionary Access Control List.
- CVE-2022-21836: Spoofing vulnerability in Windows Certificate.

Some of the critical vulnerabilities are listed below:

- CVE-2022-21846: Remote Code-Execution vulnerability in Microsoft exchange server which.
- CVE-2022-21840: Remote Code-Execution vulnerability in Microsoft Office 365.
- CVE-2022-21857: Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2022-21898: Privilege escalation vulnerability in DirectX Graphics.
- CVE-2022-21912: DirectX Graphics Kernel Remote Code Execution Vulnerability.
- CVE-2022-21907: HTTP Protocol Stack Remote Code-Execution Vulnerability
- CVE-2022-21917: HEVC Video Extensions Remote Code-Execution Vulnerability.

Out of the critical bugs, a Remote Code-Execution (CVE-2022-21907) issue in the HTTP protocol stack (HTTP.sys) used as a protocol listener for processing HTTP requests by the Windows Internet Information Services (IIS) web server. Successful exploitation requires an attacker to send maliciously crafted packets to targeted Windows servers, which use the vulnerable HTTP Protocol Stack for processing packets.
Hive Pro threat researchers recommend users to prioritize patching this flaw on all the affected servers since it could allow unauthenticated attackers to remotely execute arbitrary code in low complexity attacks and "in most situations," without requiring user interaction.

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-21846	Windows Server 2013,2016 and 2019	cpe:2.3:a:microsoft:exchange_server:2013_cu23:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2016_cu22:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019_cu11:*:*:*:*:*:*:*	Microsoft Exchange Server Remote Code Execution Vulnerability	CWE-20
CVE-2022-21840	Microsoft office 365, 2013, 2016, 2019 and 2021	cpe:2.3:a:microsoft:office:365_apps_for_enterprise:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2013_rt:sp1:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2019:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:ltsc_2021:*:*:*:*:*:*:*	Microsoft Office Remote Code Execution Vulnerability	CWE-94
CVE-2022-21917	Hevc video extensions	cpe:2.3:a:microsoft:hevc_video_extensions:*:*:*:*:*:*:*:*	HEVC Video Extensions Remote Code Execution Vulnerability.	CWE-94
CVE-2021-22947	Windows 10, 11 and Windows Server 20h2, 2019, 2022	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_11:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:*	Open-Source Curl Remote Code Execution Vulnerability	CWE-345
CVE-2022-21898	Windows 10 and Windows Server 20h2, 2019, 2022	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:*	DirectX Graphics Kernel Remote Code Execution Vulnerability	CWE-416

Hive Pro

THREAT ADVISORY

CVE ID	Affected products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-21919	Windows 7,8.1, 10, 11 and Windows Server 2008, 2012, 2016, 20h2, 2019, 2022	cpe:2.3:o:microsoft:windows_7:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_11:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:* , cpe:2.3:o:microsoft:windows_server_2008_r2:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:sp2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:* , cpe:2.3:o:microsoft:windows_server_2012_r2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:* , cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:* , cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:*	Windows User Profile Service Elevation of Privilege Vulnerability	CWE-94
CVE-2021-36976	Windows 10, 11 and Windows Server 20h2, 2019, 2022	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_11:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:* , cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:* , cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:*	Libarchive Remote Code Execution Vulnerability	CWE-416
CVE-2022-21839	Windows Server 2019 and Windows 10 1809	cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:* , cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*	Windows Event Tracing Discretionary Access Control List Denial of Service Vulnerability	CWE-20

Hive Pro

THREAT ADVISORY

CVE ID	Affected products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-21912	Windows 10 and Windows Server 20h2, 2019	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	DirectX Graphics Kernel Remote Code Execution Vulnerability	CWE-94
CVE-2022-21907	Windows 10, 11 and Windows Server 20h2, 2019, 2022	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_11:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:*	HTTP Protocol Stack Remote Code Execution Vulnerability	CWE-119
CVE-2022-21836			Microsoft Windows Certificate Privilege Escalation	CWE-451
CWE-94	Windows 10, 11 and Windows Server 2016, 2019, 2019 20H2, 2019 1709, 2019 1803, 2019 1903, 2019 1909, 2019 2004, 2022	cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_11:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008_r2:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:sp2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012_r2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:*:*:*	Remote Code-Execution vulnerability in Local Windows Security Center API	CWE-94
CVE-2022-21857			Active Directory Domain Services Elevation of Privilege Vulnerability	CWE-264

Patch Links

https://msrc.microsoft.com/update-guide/

References

https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/Jan-2022.html
https://threatpost.com/microsoft-wormable-critical-rce-bug-zero-day/177564/
https://www.bleepingcomputer.com/news/microsoft/microsoft-new-critical-windows-http-vulnerability-is-wormable/
https://www.bleepingcomputer.com/news/microsoft/microsoft-new-critical-windows-http-vulnerability-is-wormable/
https://thehackernews.com/2022/01/first-patch-tuesday-of-2022-brings-fix.html