Hive Pro

THREAT ADVISORY

Wormable vulnerability found in Windows HTTP Protocol Stack could result in malicious code execution on the OS kernel	TA202113
Threat Level Red	**Publish Date –** May 26, 2021

A wormable vulnerability (CVE-2021-31166) has been found in HTTP Protocol Stack used by the Windows Internet Information Services (IIS) affecting WinRM on Windows 10 and Server systems. An attacker can exploit this vulnerability by sending a formatted package incorrectly and running malicious code directly on the OS kernel without any authentication.

Vulnerability Details

CVE ID	Affected Versions	Affected CPEs	Vulnerability Name
CVE-2021-31166	Microsoft Windows 10 versions 2004,20h2 Microsoft Windows Server versions 2004,20h2	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:2004:*:*:*:*:*:*:*	HTTP Protocol Stack Remote Code Execution Vulnerability

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31166

References

https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31166
https://www.bleepingcomputer.com/news/security/exploit-released-for-wormable-windows-http-vulnerability/
https://www.bleepingcomputer.com/news/security/wormable-windows-http-vulnerability-also-affects-winrm-servers/
https://vuldb.com/?id.174865