Hive Pro

THREAT ADVISORY

PuzzleMaker using Chrome zero-day exploit to get into your Windows PC

TA202119

Threat Level Red

Publish Date – June 9, 2021

A chain of zero-day vulnerabilities is being used by a new threat actor, PuzzleMaker. PuzzleMaker uses a chrome V8 type confusion vulnerability(CVE-2021-21224), which allows the attacker to execute an arbitrary code via a crafted HTML page. This elevation of privilege (EoP) exploit is then used by the PuzzleMaker to get into windows 10 using the information disclosure vulnerability(CVE-2021-31955) and the heap buffer overflow vulnerability(CVE-2021-31956).
The Techniques used by the PuzzleMaker includes:
T1543 - Create or Modify System Process
T1189 - Drive-by Compromise
T1059 - Command and Scripting Interpreter
T1055 - Process Injection
T1134 - Access Token Manipulation
T1057 - Process Discovery
T1203 - Exploitation for Client Execution
T1215 - Kernel Modules and Extensions

Vulnerability Details

CVE ID	Affected Versions	Affected CPEs	Vulnerability Name	CWE ID
CVE-2021-21224	Google Chrome prior to 90.0.4430.85	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Google chrome v8 type confusion	CWE-843
CVE-2021-31955	Microsoft Windows version 10 20H2, 10 21H1,10 1809, 10 1909,10 2004, Server 20H2, Server 1909, Server 2004	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*	Microsoft Windows Kernel information disclosure	CWE-200
CVE-2021-31956	Microsoft Windows version 7 SP1,8.1, 10, 10 20H2, 10 21H1, 10 1607, 10 1809, 10 1909, 10 2004, RT 8.1, Server 20H2, Server 1909, Server 2004, Server 2008 R2 SP1, Server 2008 SP2, Server 2012, Server 2012 R2, Server 2016,Server 2019	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_10:1607:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*, 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:*:*:*:*:*:*:*:*	Microsoft Windows NTFS Remote Privilege Escalation	

Indicators of Compromise

Type	Value
Files	%SYSTEM%\WmiPrvMon.exe %SYSTEM%\wmimon.dll
MD5 Hash	09a5055db44fc1c9e3add608efff038c d6b850c950379d5ee0f254f7164833e8
SHA-1 Hash	bffa4462901b74dbfbffaa3a3db27daa61211412 e63ed3b56a5f9a1ea5c92d3d2444196ea13be94b
SHA-256 Hash	982f7c4700c75b81833d5d59ad29147c392b20c760fe36b200b541a0f841c8a9 8a17279ba26c8fbe6966ea3300fdefb1adae1b3ed68f76a7fc81413bd8c1a5f6
Domain	media-seoengine.com

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31956
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31955
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_20.html

References

https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/
https://otx.alienvault.com/pulse/60c088d3fd6e59ee86c1b78b