Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

Spyware Group Candiru exploits Chrome Zero-Day to Target Middle East

Date of Publication	Admiralty Code	TA Number
July 27, 2022	A1	TA2022157

Summary

Candiru(Saito Tech) spyware used the recently fixed CVE-2022-2294 Chrome zero-day in assaults on journalists, with a substantial portion of the attacks taking place in Lebanon. This recently patched vulnerability in WebRTC is a heap-based buffer overflow. Its successful exploitation may result in code execution on the targeted device.

CVE Table

CVE	NAME	PATCH
CVE-2022-2294	Heap buffer overflow in WebRTC	✓

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**T1055** Process Injection	**TA0004** Privilege Escalation	**TA0009** Collection
T1560 Archive Collected Data	**TA0002** Execution	**T1203** Exploitation for Client Execution	**T1014** Rootkit
TA0043 Reconnaissance	**T1589** Gather Victim Identity Information	**T1592** Gather Victim Host Information	

Technical Details

#1

The adversaries have used watering hole attacks employing Google Chrome zero-day exploits to target users in Lebanon, Turkey, Yemen, and Palestine. The compromised website included evidence of persistent XSS attacks, which the attacker ultimately exploited by injecting code that redirected the victims to attacker-controlled domains.

#2

Candiru collects additional information once the victim reaches the exploit server. A profile of the victim's browser is compiled and delivered to the attackers. It consists of about 50 data points, the victim's Language, timezone, screen information, device type, browser plugins, referrer, device memory, cookie functioning, and more.

#3

Following the initial infection, the malicious payload known as DevilsTongue spyware attempts to enter the kernel by targeting a legitimately signed kernel driver in a BYOVD (Bring Your Own Vulnerable Driver) fashion to elevate privileges and gain read and write access to the memory of the infected device.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-2294	Google Chrome: 70.0.3538.67 - 103.0.5060.66	cpe:2.3:a:google:google_chrome:*:*:*:*:*:*:*:*	CWE-122

Indicator of Compromise (IOC)

TYPE	VALUE
Domains	bad-shop[.]net bestcarent[.]org core-update[.]com datanalytic[.]org expertglobal[.]org only-music[.]net popsonglist[.]com querylight[.]net smartstand[.]org stylishblock[.]com webs-update[.]com
File Path	C:\Windows\System32\migration\netiopmig.dll C:\Windows\System32\migration\sppvmig.dll C:\Windows\System32\migration\spvmig.dll C:\Windows\System32\ime\imejp\imjpueact.dll C:\Windows\System32\ime\imejp\imjpuexp.dll C:\Windows\System32\ime\imetc\imtcprot.dll C:\Windows\System32\ime\shared\imccphd.dll C:\Windows\System32\ime\shared\imebrokev.dll C:\Windows\System32\ime\shared\imecpmeid.dll C:\Windows\System32\ime\shared\imepadsvd.dll C:\Windows\System32\migration\imjprmig.dll C:\Windows\System32\wbem\dmwmibridgeprov132.dll C:\Windows\System32\wbem\esscli32.dll C:\Windows\System32\wbem\netdacim32.dll C:\Windows\System32\wbem\netpeerdistcim32.dll C:\Windows\System32\wbem\viewprov32.dll C:\Windows\System32\wbem\vsswmi32.dll C:\Windows\System32\wbem\wbemcore32.dll C:\Windows\System32\wbem\wbemdisp32.dll C:\Windows\System32\wbem\wbemsvc32.dll C:\Windows\System32\wbem\wfascim32.dll C:\Windows\System32\wbem\win32_encryptablevolume32.dll C:\Windows\System32\wbem\wmiaprpl32.dll C:\Windows\System32\drivers\HW.sys C:\Windows\System32\drivers\HW.sys.dat

TYPE	VALUE
Registry keys	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32, HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{4FA18276-912A-11D1-AD9B-00C04FD8FDFF}\InprocServer32, HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InProcServer32, HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32

Patch Details

Update to Google Chrome version 103.0.5060.114 for Windows, MacOS, and Linux.

References

https://decoded.avast.io/janvojtesek/the-return-of-candiru-zero-days-in-the-middle-east/

https://www.hivepro.com/zero-day-vulnerability-in-chrome-browser-being-exploited-in-the-wild/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 27, 2022 • 3:38 AM

More at www.hivepro.com