

THREAT ADVISORY

Environment Variables Leak affect Multiple browsers**TA2022069****Threat Level****AMBER****Publish Date –March 21, 2022**

A system environment variables leak security bug was found in Chromium 92 version. Multiple web browsers are based on the chromium engine, such as Google Chrome, Microsoft Edge, Opera, and Brave. Most of them are reported to be vulnerable, except Brave.

The vulnerability tracked as CVE-2022-0337 affects the 'window.showSaveFilePicker()' method in the File system access API. An attacker can exploit this vulnerability to gain access to the victim's system environment variables by crafting a malicious html file and enticing a victim user to open it. Environment variables are the variables where users can store secrets like tokens, passwords, keys to some services (ex. Microsoft Azure or Twilio SendGrid). This vulnerability only affects Windows operating system.

Potential MITRE ATT&CK TTPs are:

TA0042: Resource Development

T1588: Obtain Capabilities

T1588.006: Obtain Capabilities: Vulnerabilities

TA0001: Initial Access

T1190: Exploit Public-Facing Application

TA0005: Defense Evasion

T1027: Obfuscated Files or Information

T1027.006: Obfuscated Files or Information: HTML Smuggling

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0337	Google chrome prior to version 97, Microsoft Edge(chromium version) prior to version 97, Opera prior to version 82	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* *:* cpe:2.3:a:microsoft:edge:- :*:*:*:*:*:*:* cpe:2.3:a:opera:opera_browser:*:* *:*:*:*:*	Inappropriate implementation in File System API	CWE-358

Patch Link

<https://www.google.com/intl/en/chrome/?standalone=1>

https://download3.operacdn.com/pub/opera/desktop/84.0.4316.42/win/Opera_84.0.4316.42_Setup_x64.exe

<https://www.microsoft.com/en-us/edge>

References

<https://github.com/Puliczek/CVE-2022-0337-PoC-Google-Chrome-Microsoft-Edge-Opera>

<https://chromereleases.googleblog.com/2022/01/stable-channel-update-for-desktop.html>