Win32k Privilege Escalation

A Microsoft vulnerability added to CISA-300 on Feb 4, 2022

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21882

CVEs: CVE-2022-21882

Public exploit code was disclosed and CISA requires all federal agencies to patch all systems vulnerable to CVE-2022-21882 by Feb 18, 2022.

Background

A local, authenticated attacker could gain elevated local system or administrator privileges through a vulnerability in the Win32k.sys driver. CISA has added to the list of known publically exploited vulnerabilities on February 4, 2022.

Announced

Announced and fix published by Microsoft on January 11 as part of patch Tuesday -

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21882

.

Latest Developments

As per a binding operational directive (BOD 22-01) issued in November and today's announcement, all Federal Civilian Executive Branch Agencies (FCEB) agencies are now required to patch all systems against this vulnerability within two weeks, until February 18th. While BOD 22-01 only applies to FCEB agencies, CISA strongly urges all private and public sector organizations to reduce their exposure to ongoing cyberattacks by adopting this Directive and prioritizing mitigation of vulnerabilities included in its catalog of actively exploited security flaws.

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**IPS**	*19.244*	Blocks attempts to exploit CVE-2022-21882
FortiClient	**Vulnerability**	*1.287*	Detects the presence of Win32k vulnerability CVE-2022-21882, and applies auto-patching if enabled.
FortiSASE	**IPS**	*19.244*	Blocks attempts to exploit CVE-2022-21882
FortiADC	**IPS**	*19.244*	Blocks attempts to exploit CVE-2022-21882
FortiProxy	**IPS**	*19.244*	Blocks attempts to exploit CVE-2022-21882
FortiAnalyzer	**Outbreak Detection**	*1.049*	Detects indicators for the CVE-2022-21882 vulnerability across the Security Fabric
	Threat Hunting	*6.4+*	Detects indicators for the CVE-2022-21882 vulnerability across the Security Fabric

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiClient

Vulnerability
Version Info: 1.287
Link: https://www.fortiguard.com/updates/epvuln?version=1.287

Exploitation

FortiGate

IPS
Version Info: 19.244
Link: https://www.fortiguard.com/updates/ips?version=19.244

FortiSASE

IPS
Version Info: 19.244
Link: https://www.fortiguard.com/updates/ips?version=19.244

FortiADC

IPS
Version Info: 19.244
Link: https://www.fortiguard.com/updates/ips?version=19.244

FortiProxy

IPS
Version Info: 19.244
Link: https://www.fortiguard.com/updates/ips?version=19.244

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer

Outbreak Detection
Version Info: 1.049
Link: https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00049

Threat Hunting
Version Info: 6.4+
Link: https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-Win32k-sys-driver/ta-p/204467