

Microsoft Win32k Privilege Escalation Vulnerability

Critical vulnerability affecting some unknown functionality of the component Win32k

<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 publicly 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.

PROTECT


Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery
- Vulnerability
 - Detects the presence of Win32k vulnerability CVE-2022-21882, and applies auto-patching if enabled.
 - 

FortiClient

DB 1.287
- Exploitation
 - IPS
 - Blocks attempts to exploit CVE-2022-21882
 - 

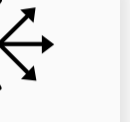
FortiGate

DB 19.244
 - 

FortiSASE

DB 19.244
 - 

FortiNDR

DB 19.244
 - 

FortiADC

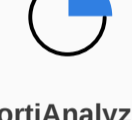
DB 19.244
 - 

FortiProxy

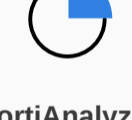
DB 19.244
- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

- Outbreak Detection
 - 

FortiAnalyzer

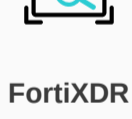
DB 1.00049
- Threat Hunting
 - 


FortiAnalyzer

v6.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:


- Automated Response
 - Services that can automatically respond to this outbreak.
 - 


FortiXDR
- Assisted Response Services
 - Experts to assist you with analysis, containment and response activities.
 - 


Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

- NOC/SOC Training
 - Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.
 - 


NSE Training
 - 

Response Readiness
- End-User Training
 - Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.
 - 

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

- Attack Surface Hardening
 - Check Security Fabric devices to build actionable configuration recommendations and key indicators.
 - 

Security Rating

Additional Resources

CISA Alert <https://www.cisa.gov/uscert/ncas/current-activity/2021/02/09/microsoft-warns-windows-win32k-privilege-escalation>

Bleeping computer <https://www.bleepingcomputer.com/news/microsoft/windows-vulnerability-with-new-public-exploits-lets-you-become-admin/>

Threat Post <https://threatpost.com/cisa-orders-federal-agencies-to-fix-actively-exploited-windows-bug/178270/>

Learn more about [FortiGuard Outbreak Alerts](#)