F#RTINET. **OUTBREAK ALERTS**

Microsoft Outlook Elevation of Privilege Vulnerability No-interaction, zero day vulnerability exploited in the wild

https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/ CVEs: CVE-2023-23397

CVE-2023-23397 is a critical elevation of privilege (EoP) vulnerability in Microsoft Outlook. It is a zero-touch exploit, meaning the security flaw

Outlook such as Android, iOS, Mac, as well as Outlook on the web. **Background** CVE-2023-23397 is a critical privilege elevation/authentication bypass vulnerability in Outlook, released as part of

escalate privileges, or further compromise the environment.

requires no user interaction to be abused. All supported versions of Microsoft Outlook for Windows are affected including other versions of Microsoft

which again, does not need to be opened. From here, attackers may capture Net-NTLMv2 hashes, which enable authentication in Windows environments. This allows threat actors to potentially authenticate themselves and

Announced March 14, 2023: Microsoft Mitigates Outlook Elevation of Privilege Vulnerability https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/

2023-23397.md

March 24, 2023: Microsoft released guidance for investigating attacks using CVE-2023-23397

Latest Developments https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/

> FortiGuard Labs recommends users to follow vendor guidelines for patching affected versions of Outlook. Microsoft has also provided a PowerShell script designed to scan emails, calendar entries, and task items, and to verify if they have the malicious property.

the March Patch Tuesday set of fixes. Threat actors are exploiting this vulnerability by sending a malicious email

https://github.com/microsoft/CSS-Exchange/blob/a4c096e8b6e6eddeba2f42910f165681ed64adf7/docs/Security/CVE-

PROTECT

Reconnaissance Weaponization

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

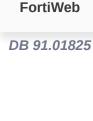
Delivery

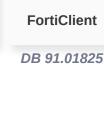
AV

Detects and blocks known malware payloads related to CVE-2023-23397

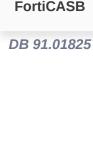


DB 91.01825













Vulnerability

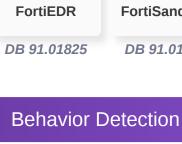
DB 1.418

AV (Pre-filter)

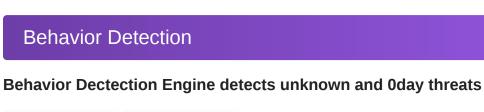
FortiSandbox FortiNDR

DB 91.01825

Detects and blocks known malware payloads related to CVE-2023-23397

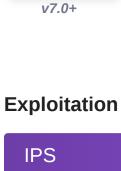


FortiSandbox





Anti-spam



DB 23.518

FortiGate





FortiSASE

DB 23.518

Detects and blocks attack attempts related to CVE-2023-23397

FortiNDR

DB 23.518

FortiADC

DB 23.518

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

FortiProxy

DB 23.518



DB 0.02506 DB 0.02506

alert and generate reports:

FortiSIEM

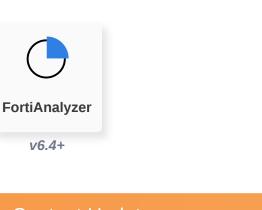
FortiSOCaaS

DB 0.02506



FortiSIEM DB 313

Outbreak Detection



Assisted Response Services

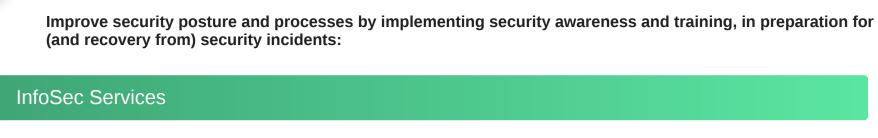
Automated Response

FortiRecon:

RECOVER

Services that can automatically respond to this outbreak.

Develop containment techniques to mitigate impacts of security events:



Security readiness and awareness training for SOC teams, InfoSec and general employees.

IDENTIFY

Identify processes and assets that need protection: Attack Surface Monitoring (Inside & Outside)







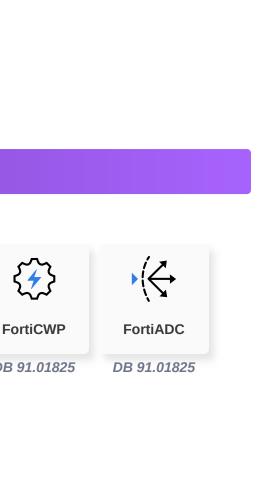
FortiRecon:

EASM

https://www.securityweek.com/microsoft-no-interaction-outlook-zero-day-exploited-since-last-april/ https://thestack.technology/critical-microsoft-outlook-vulnerability-cve-2023-23397/

2022/ **The Hacker News** https://thehackernews.com/2023/03/microsoft-warns-of-stealthy-outlook.html

Learn more about FortiGuard Outbreak Alerts



Detects vulnerable instances of Microsoft Outlook (CVE-2023-23397) FortiClient

DB 91.01825

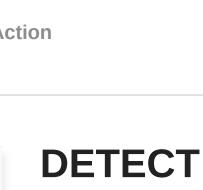
v4.0+ v7.0+

Detects and filters spam from mailboxes



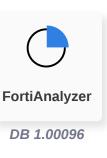
FortiMail







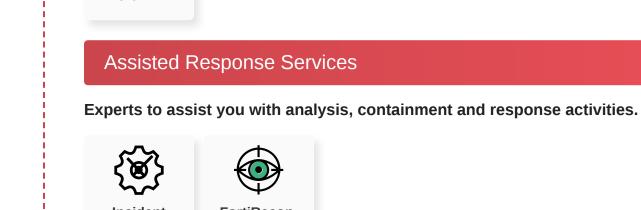
IOC



Threat Hunting

Content Update

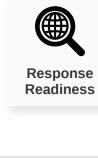




FortiXDR

Response















F#RTINET

Security Week

Bleeping Computer

The Stack