FORTINET

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 requires no user interaction to be abused. All supported versions of Microsoft Outlook for Windows are affected including other versions of Microsoft 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 the March Patch Tuesday set of fixes. Threat actors are exploiting this vulnerability by sending a malicious email 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 escalate privileges, or further compromise the environment.

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/

Latest Developments

March 24, 2023: Microsoft released guidance for investigating attacks using CVE-2023-23397
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.
https://github.com/microsoft/CSS-Exchange/blob/a4c096e8b6e6eddeba2f42910f165681ed64adf7/docs/Security/CVE-2023-23397.md
.

PROTECT

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

Reconnaissance

Weaponization

Delivery

AV

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

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiCASB	FortiCWP	FortiADC	FortiProxy
DB 91.01825	DB 91.01825	DB 91.01825	DB 91.01825	DB 91.01825	DB 91.01825	DB 91.01825	DB 91.01825

Vulnerability

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

FortiClient
DB 1.418

AV (Pre-filter)

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

FortiEDR	FortiSandbox	FortiNDR
DB 91.01825	DB 91.01825	DB 91.01825

Behavior Detection

Behavior Dectection Engine detects unknown and 0day threats

FortiSandbox	FortiMail
v4.0+	v7.0+

Anti-spam

Detects and filters spam from mailboxes

FortiMail
v7.0+

Exploitation

IPS

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

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 23.518	DB 23.518	DB 23.518	DB 23.518	DB 23.518

Installation

C2

Action

DETECT

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

IOC

FortiAnalyzer	FortiSIEM	FortiSOCaaS
DB 0.02506	DB 0.02506	DB 0.02506

Outbreak Detection

FortiAnalyzer
DB 1.00096

Threat Hunting

FortiAnalyzer
v6.4+

Content Update

FortiSIEM
DB 313

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly respond to this outbreak.

- FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

- Incident Response
- FortiRecon: ACI

RECOVER

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

InfoSec Services

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

- Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

- Security Rating
- FortiRecon: EASM

Additional Resources

FortiGuard Threat Signal	https://www.fortiguard.com/threat-signal-report/5061
Security Week	https://www.securityweek.com/microsoft-no-interaction-outlook-zero-day-exploited-since-last-april/
The Stack	https://thestack.technology/critical-microsoft-outlook-vulnerability-cve-2023-23397/
Bleeping Computer	https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-outlook-zero-day-used-by-russian-hackers-since-april-2022/
The Hacker News	https://thehackernews.com/2023/03/microsoft-warns-of-stealthy-outlook.html

Learn more about FortiGuard Outbreak Alerts

FORTINET