



CVE-2022-41040

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-41040

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

S:S31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/R



Certain versions of [Exchange Server](#) from [Microsoft](#) contain the following vulnerability:

Microsoft Exchange Server Elevation of Privilege Vulnerability.

CVE-2022-41040 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Microsoft - Microsoft Exchange Server 2013 version Cumulative Update 23**

Affected Vendor/Software: **Microsoft - Microsoft Exchange Server 2016 Cumulative Update 22 version**

Affected Vendor/Software: **Microsoft - Microsoft Exchange Server 2019 Cumulative Update 11 version**

Affected Vendor/Software: **Microsoft - Microsoft Exchange Server 2019 Cumulative Update 12 version**

Affected Vendor/Software: **Microsoft - Microsoft Exchange Server 2016 Cumulative Update 23 version**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Microsoft November 2022 Patch Tuesday fixes 65 vulnerabilities!	www.secpod.com text/html	MISC www.secpod.com/blog/microsoft-november-2022-patch-tuesday-patches-65-vulnerabilities-including-6-zero-days/
VU#915563 - Microsoft Exchange vulnerable to server-	www.kb.cert.org	CERT-VN VU#915563

side request forgery and remote code execution.	text/html	
Security Update Guide - Microsoft Security Response Center	portal.msrc.microsoft.com text/html	MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040
Microsoft Exchange ProxyNotShell Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/170066/Microsoft-Exchange-ProxyNotShell-Remote-Code-Execution.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- [150664](#) Microsoft Exchange Server Multiple Vulnerabilities (ProxyNotShell) (CVE-2022-41040,CVE-2022-41082)
- [48223](#) Microsoft Exchange Server Multiple Vulnerabilities Mitigation Applied (ProxyNotShell)
- [50122](#) Microsoft Exchange Server Multiple Vulnerabilities (Zero Day)(ProxyNotShell)
- [730621](#) Microsoft Exchange Server Multiple Vulnerabilities (ProxyNotShell) (Unauthenticated Check)

Exploit/POC from Github

Mass exploitation tool for ProxyNotShell (CVE-2022-41082/CVE-2022-41040) supports multi threading and written in python

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2013	cumulative_update_23	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_22	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_23	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_11	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_12	All	All
cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:						
cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_22:*:*:*:*:						
cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_23:*:*:*:*:						
cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_11:*:*:*:*:						
cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_12:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @caniffe	@GossiTheDog CVE-2022-41040 / CVE-2022-41082 - msrc-blog.microsoft.com/2022/09/29/cus...	2022-09-30 07:20:15
 @TrendMicroRSRCH	UPDATE: Microsoft has released a blog acknowledging the two zero-days and assigned these CVEs: CVE-2022-41040 and C... twitter.com/i/web/status/1...	2022-09-30 08:08:40
 @TrendMicroRSRCH	UPDATE: Microsoft has released a blog acknowledging the two zero-days and assigned these CVEs: CVE-2022-41040 and... twitter.com/i/web/status/1...	2022-09-30 08:09:59
 @hasegawayosuke	Exchange Serverのゼロデイ(CVE-2022-41040、CVE-2022-41082)のやつ、MSから軽減策の案内出た。 / Customer Guidance for Reported Zero-day Vuln... twitter.com/i/web/status/1...	2022-09-30 08:26:49
 @GossiTheDog	For example, if you have SSRF (CVE-2022-41040) you are god in Exchange, and can access any mailbox via EWS - see th... twitter.com/i/web/status/1...	2022-09-30 08:32:20
 @Swati_THN	#Microsoft confirms that 2 new zero-day vulnerabilities (CVE-2022-41040, CVE-2022-41082) affecting Exchange Server... twitter.com/i/web/status/1...	2022-09-30 09:26:00
 @AcooEdi	CVE-2022-41040 & CVE-2022-41082: Exchange Server Zero-Days Under Attack dlvr.it/SZG8BD via securityonline https://t.co/PxOsWENI3Q	2022-09-30 09:28:34
 /r/HackProtectSlo	Ranljivost Micosoft Exchange strežnika	2022-09-30 13:25:28
 /r/crowdstrike	SITUATIONAL AWARENESS // ProxyNotShell // CVE-2022-40140 & CVE-2022-41082	2022-10-01 13:56:35
 /r/blueteamsec	Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082 - the new Exchange vulns - < 10 orgs globally	2022-10-01 16:32:31
 /r/SecOpsDaily	Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082 - Microsoft Security Blog	2022-10-01 17:51:30
 /r/u/Suitable_Air	ProxyNotShell: Detecting CVE-2022-41040 and CVE-2022-41082, Novel Microsoft Exchange Zero-Day Vulnerabilities Actively Exploited in the Wild	2022-10-01 17:30:41
 /r/netcve	CVE-2022-41040	2022-10-03 01:38:33
 /r/fortinet	ProxyNotShell Exchange and the Fortigate IPS	2022-10-03 15:19:14
 /r/worldTechnology	Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082 - Microsoft Security Blog	2022-10-03 21:15:55
 /r/networking	CVE-2022-41082 and CVE-2022-41040 related to Zero-day Vulnerabilities in Microsoft Exchange Server	2022-10-04 11:36:47
 /r/u/serverprotips	Microsoft Exchange CVE-2022-41040 Mitigation with EOMTv2	2022-10-06 19:41:20
 /r/sysadmin	Anyone notice that MS URL Rewrite for CVE-2022-41040, CVE-2022-41082 isn't quite working?	2022-10-06 19:19:39
 /r/exchangeserver	Testing ProxyNotShell (CVE-2022-41040; CVE-2022-41082) mitigation?	2022-10-07 17:43:13
 /r/Serverprotips	Microsoft Exchange CVE-2022-41040 Mitigation with EOMTv2 - ServerProTips	2022-10-08 21:36:15
 /r/sysadmin	Is it possible to see when a IIS rewrite rule was created?	2022-10-10 07:54:05
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Critical Patches Issued for Microsoft Products, October 11, 2022 - PATCH: NOW	2022-10-12 13:09:24

 /r/ITNoobs	What does this mean? Zero-day Vulnerabilities in Microsoft Exchange Server	2022-10-13 13:14:46
 /r/exchangeserver	Side effects of disabling OWA for cve 2022-41040 41082 and reversible method	2022-10-13 19:18:30
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Critical Patches Issued for Microsoft Products, November 8, 2022 - PATCH: NOW	2022-11-09 13:58:02
 /r/u/R00t3dNations	Utiliza NMAP para Verificar la Vulnerabilidad CVE-2022-41040 - ProxyNotShell	2022-11-14 04:34:32
 /r/blueteamsec	ProxyNotShell-PoC: Working PoC for CVE-2022-41040 and CVE-2022-41082 (A.K.A ProxyNotShell) - aka Exchange in the wild 0day	2022-11-17 04:40:13
 /r/KibernetinisSaugumas	Du pavojingus "Microsoft Exchange Server" pažeidžiamumus naudojantis PoC išnaudojimo kodas jau internete	2022-11-21 11:37:09
 /r/HackProtectSlo	Top 10 exploited vuln 2022	2022-12-07 17:32:06
 /r/netsecnews	CVE-2022-41040 and CVE-2022-41082 – zero-days in MS Exchange	2022-12-19 17:35:38
 /r/UIC	CVE-2022-41040 and CVE-2022-41082 – zero-days in MS Exchange	2022-12-19 17:35:13
 /r/blueteamsec	CVE-2022-41040 and CVE-2022-41082 – zero-days in MS Exchange	2022-12-20 12:10:21
 /r/bugbounty	CVE-2022-41040: ProxyNotShell Exchange Vulnerability	2023-01-09 10:24:09

[← Previous ID](#)
[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)