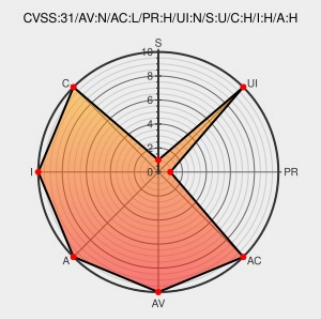
CVE-2020-16875

Published on: 09/11/2020 12:00:00 AM UTC

Last Modified on: 04/28/2022 06:32:00 PM UTC

CVE-2020-16875

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Exchange Server from Microsoft contain the following vulnerability:

A remote code execution vulnerability exists in Microsoft Exchange server due to improper validation of cmdlet arguments.An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user, aka 'Microsoft Exchange Server Remote Code Execution Vulnerability'.

CVE-2020-16875 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Microsoft** - **Microsoft Exchange Server 2019 Cumulative Update 5** version

Affected Vendor/Software: **Microsoft** - **Microsoft Exchange Server 2019 Cumulative Update 6** version

Affected Vendor/Software: **Microsoft** - **Microsoft Exchange Server 2016 Cumulative Update 16** version

Affected Vendor/Software: **Microsoft** - **Microsoft Exchange Server 2016 Cumulative Update 17** version

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Microsoft Exchange Server DlpUtils AddTenantDlpPolicy Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159210/Microsoft-Exchange-Server-DlpUtils-AddTenantDlpPolicy-Remote-Code-Execution.html
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	N/A N/A

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2016	cumulative_update_16	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_17	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_5	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_6	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_16	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_17	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_5	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_6	All	All

cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_16:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_17:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_5:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_6:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_16:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_17:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_5:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@itbezopasnost	Охота на атаки MS Exchange. Часть 2 (CVE-2020-0688, CVE-2020-16875 и CVE-2021-24085) ift.tt/3oPmPYp	2021-05-26 10:20:21
@ITnan_ru	Охота на атаки MS Exchange. Часть 2 (CVE-2020-0688, CVE-2020-16875 и CVE-2021-24085): itnan.ru/p/?p=1559208 https://t.co/1zx3AQAxk1	2021-05-26 10:35:03
@is_n3ws	Охота на атаки MS Exchange. Часть 2 (CVE-2020-0688, CVE-2020-16875 и CVE-2021-24085) ift.tt/3oPmPYp https://t.co/djCwoI9fjz	2021-05-26 11:12:17
@gebutcher	Охота на атаки MS Exchange. Часть 2 (CVE-2020-0688, CVE-2020-16875 и CVE-2021-24085) habr.com/ru/post/559208/… twitter.com/i/web/status/1…	2021-05-26 11:32:46
@nanothyll	Hunting Down MS Exchange Attacks. Part 2 (CVE-2020-0688, CVE-2020-16875, CVE-2021-24085) cyberpolygon.com/materials/okho…	2021-06-23 16:19:34
@blueteamsec1	Hunting Down MS Exchange Attacks. Part 2 (CVE-2020-0688, CVE-2020-16875, CVE-2021-24085) dlvr.it/S3L6rw… twitter.com/i/web/status/1…	2021-07-08 18:54:07
@ipssignatures	The vuln CVE-2020-16875 has a tweet created 2 days ago and retweeted 10 times. twitter.com/blueteamsec1/s… #pow1rtrtwwcve	2021-07-10 23:06:00
@kaidja	@cyb3rops cyberpolygon.com/materials/okho…	2021-08-12 13:44:11
@psyopsnewsSWE	cyberpolygon.com/materials/okho…	2023-03-04 00:17:14
/r/purpleteamsec	Hunting Down MS Exchange Attacks. Part 2 (CVE-2020–0688, CVE-2020–16875, CVE-2021–24085)	2021-06-16 22:12:15
/r/purpleteamsec	Hunting Down MS Exchange Attacks. Part 2 (CVE-2020-0688, CVE-2020-16875, CVE-2021-24085)	2021-06-23 15:02:41
/r/blueteamsec	Hunting Down MS Exchange Attacks. Part 2 (CVE-2020-0688, CVE-2020-16875, CVE-2021-24085)	2021-06-23 14:58:08

← Previous ID

Next ID→