CVE-2018-8581

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-8581
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-14 01:29:00 UTC
Updated	2020-04-09 13:16:00 UTC
Description	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka "Microsoft Exchange Server Elevation of Priv

Risk And Classification

EPSS: 0.914990000 probability, percentile 0.996770000 (date 2026-05-08)

CISA KEV: Listed on 2022-03-03; due 2022-03-17; ransomware use Known

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Exchange Server
Name	Microsoft Exchange Server Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-8581

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2010	-	All	All
Application	Microsoft	Exchange Server	2013	-	All	All
Application	Microsoft	Exchange Server	2016	-	All	All
Application	Microsoft	Exchange Server	2019	-	All	All
Application	Microsoft	Exchange Server	2010	-	All	All
Application	Microsoft	Exchange Server	2013	-	All	All
Application	Microsoft	Exchange Server	2016	-	All	All
Application	Microsoft	Exchange Server	2019	-	All	All

References

Reference	Source	Link
Microsoft Exchange Server CVE-2018-8581 Remote Privilege Escalation Vulnerability	BID	www.securityfocus.com
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8581	CONFIRM	portal.msrc.microsoft.com
Microsoft Exchange Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www.securitytracker.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**