CVE-2021-34523

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

Summary

CVE	CVE-2021-34523
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-14 18:15:00 UTC
Updated	2023-12-28 23:15:00 UTC
Description	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768, CVE-2021-34

Risk And Classification

EPSS: 0.939980000 probability, percentile 0.998940000 (date 2026-05-10)

CISA KEV: Listed on 2021-11-03; due 2021-11-17; ransomware use Known

Problem Types: CWE-287

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-2021-34523

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2013	cumulative_update_23	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_19	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_20	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_8	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_9	All	All

References

Reference	Source	Link	Tags

Security Update Guide - Microsoft Security Response Center	MISC	portal.msrc.microsoft.com	
Microsoft Exchange ProxyShell Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
ZDI-21-822 | Zero Day Initiative	MISC	www.zerodayinitiative.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

50112 Microsoft Exchange Server Multiple Vulnerabilities July 2021

50114 Microsoft Exchange Server Multiple Vulnerabilities (ProxyShell) (unauthenticated)