CVE-2018-8302

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

Summary

CVE	CVE-2018-8302
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-15 17:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle obje

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2010	sp3	All	All
Application	Microsoft	Exchange Server	2013	cumulative_update_20	All	All
Application	Microsoft	Exchange Server	2013	cumulative_update_21	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_10	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_9	All	All
Application	Microsoft	Exchange Server	2010	sp3	All	All
Application	Microsoft	Exchange Server	2013	cumulative_update_20	All	All
Application	Microsoft	Exchange Server	2013	cumulative_update_21	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_10	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_9	All	All

References

Reference	Source
Microsoft Exchange CVE-2018-8302 Remote Memory Corruption Vulnerability	BID
Microsoft Exchange E-mail Processing Flaw Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	SECTRAC
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8302	CONFIRM
CVE Program record	CVE.ORG

NVD vulnerability detail NVD

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**