



# CVE-2018-8302

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

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

## 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

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

**Free CVE JSON API** [cve.report/api](#)

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