



CVE-2018-8153

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-8153
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-09 19:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web Access (OWA) fails to properly handle web

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2016	cumulative_update_8	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_9	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_8	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_9	All	All

References

Reference

- Microsoft Exchange Server CVE-2018-8153 Spoofing Vulnerability
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8153
- Microsoft Exchange Server Multiple Flaws Let Remote Users Spoof Content, Inject Scripting Code, Obtain Potentially Sensitive Information, and More
[CVE Program record](#)
- [NVD vulnerability detail](#)

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](#)