



CVE-2018-8305

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-8305
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-11 00:29:00 UTC
Updated	2018-09-08 12:06:00 UTC
Description	An information disclosure vulnerability exists in Windows Mail Client when a message is opened, aka "Windows Mail Client

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Application	Microsoft	Windows Calendar	-	All	All	All
Application	Microsoft	Windows Calendar	-	All	All	All
Application	Microsoft	Windows Mail	-	All	All	All
Application	Microsoft	Windows Mail	-	All	All	All
Application	Microsoft	Windows People	-	All	All	All
Application	Microsoft	Windows People	-	All	All	All

References

Reference
104618
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8305
Windows Mail Client Embedded URL Processing Flaw Lets Remote Users Obtain Potentially Sensitive IP Address Information on the Target S
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](#).

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