



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

CVE	CVE-2017-17847
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-27 17:08:00 UTC
Updated	2023-11-07 02:41:00 UTC
Description	An issue was discovered in Enigmail before 1.9.9. Signature spoofing is possible because the UI does not properly distinguish between the 'From' and 'To' fields in the 'Signature' field. This allows an attacker to spoof the 'From' field and send an email that appears to be from a trusted source. The issue was discovered by [REDACTED] and [REDACTED].

Problem Types: CWE-347

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Enigmail	Enigmail	All	All	All	All
Application	Enigmail	Enigmail	All	All	All	All

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-4070-1 enigmail	DEBIAN	www.debian.org	Third Party
enigmail.net/download/other/Enigmail%20Pentest%20Report%20by%20Cure53%20-%20...	MISC	enigmail.net	Vendor Adv
Re: [Enigmail] [ANN] Enigmail v1.9.9 available		www.mail-archive.com	
Enigmail / Bugs / #709 Signature Spoofing Attacks using multipart/related	MISC	sourceforge.net	Third Party
[SECURITY] [DLA 1219-1] enigmail security update	MLIST	lists.debian.org	
[SECURITY] [DSA 4070-1] enigmail security update	MISC	lists.debian.org	Third Party
Re: [Enigmail] [ANN] Enigmail v1.9.9 available	MISC	www.mail-archive.com	Mailing List,
CVE Program record	CVE.ORG	www.cve.org	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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