



CVE-2011-3355

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

Summary

CVE	CVE-2011-3355
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-25 23:15:00 UTC
Updated	2019-12-14 14:28:00 UTC
Description	evolution-data-server3 3.0.3 through 3.2.1 used insecure (non-SSL) connection when attempting to store sent email messa

Risk And Classification

Problem Types: CWE-311

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Evolution-data-server3	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

References

Reference	Source
707848 – (CVE-2011-3355) CVE-2011-3355 evolution: IMAP does non-SSL connection when storing to Sent folder	MISC
oss-security - CVE Request -- evolution -- Uses insecure (non-SSL) connection when storing the sent message into the Sent folder	MISC
CVE-2011-3355 - Red Hat Customer Portal	MISC
#641052 - evolution uses insecure connection when storing the sent message to the sent folder - Debian Bug report logs	MISC
CVE-2011-3355	MISC
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

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](#)