



# CVE-2013-0250

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

## Summary

<b>CVE</b>	CVE-2013-0250
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-06-06 14:55:00 UTC
<b>Updated</b>	2014-06-09 13:34:00 UTC
<b>Description</b>	The init_nss_hash function in exec/totemcrypto.c in Corosync 2.0 before 2.3 does not properly initialize the HMAC key, whi

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Corosync	Corosync	2.0.0	All	All	All
Application	Corosync	Corosync	2.0.1	All	All	All
Application	Corosync	Corosync	2.0.2	All	All	All
Application	Corosync	Corosync	2.0.3	All	All	All
Application	Corosync	Corosync	2.1.0	All	All	All
Application	Corosync	Corosync	2.1.1	All	All	All
Application	Corosync	Corosync	2.2.0	All	All	All
Application	Corosync	Corosync	2.0.0	All	All	All
Application	Corosync	Corosync	2.0.1	All	All	All
Application	Corosync	Corosync	2.0.2	All	All	All
Application	Corosync	Corosync	2.0.3	All	All	All
Application	Corosync	Corosync	2.1.0	All	All	All
Application	Corosync	Corosync	2.1.1	All	All	All
Application	Corosync	Corosync	2.2.0	All	All	All

## References

**Reference**

oss-sec: Re: CVE Request -- Corosync (2.0 <= X < 2.3): Remote DoS due improper HMAC initialization

totemcrypto: fix hmac key initialization · corosync/corosync@b3f456a · GitHub

oss-sec: Re: Re: CVE Request -- Corosync (2.0 <= X < 2.3): Remote DoS due improper HMAC initialization

oss-sec: CVE Request -- Corosync (X < 2.0.3): Remote DoS due improper HMAC initialization and improper junk filtering when different encry

Security Advisory SA52037 - Corosync HMAC Initialization Denial of Service Vulnerability - Secunia

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](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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)