



# CVE-2011-5034

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

## Summary

<b>CVE</b>	CVE-2011-5034
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-12-30 01:55:00 UTC
<b>Updated</b>	2023-11-07 02:09:00 UTC
<b>Description</b>	Apache Geronimo 2.2.1 and earlier computes hash values for form parameters without restricting the ability to trigger hash

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	1.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	1.1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	1.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.0.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.0.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.3	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.4	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.5	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.6	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.7	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.8	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	1.0	All	All	All

Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	1.1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	1.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.0.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.0.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.3	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.4	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.5	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.6	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.7	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.1.8	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	2.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Geronimo</a>	All	All	All	All

## References

Reference	Source	Link
Apache Geronimo Web Form Hash Collision Denial of Service Vulnerability - Secunia.com	SECUNIA	<a href="#">secunia.com</a>
[geronimo-dev] 20210727 [jira] [Created] (GERONIMO-6814) Improve Geronimo specs to mitigate CVE-2011-5034		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
[geronimo-dev] 20210727 [jira] [Commented] (GERONIMO-6814) Improve Geronimo specs to mitigate CVE-2011-5034		<a href="#">lists.apache.org</a>
[axis-java-dev] 20210623 [jira] [Resolved] (AXIS2-6004) AXIS 2 1.7.9 geronimo jars with vulnerability CVE-2011-5034		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
[karaf-issues] 20210723 [jira] [Assigned] (KARAF-7227) Upgrade geronimo artifacts to mitigate CVE-2011-5034		<a href="#">lists.apache.org</a>
[axis-java-dev] 20210622 [jira] [Updated] (AXIS2-6004) AXIS 2 1.7.9 geronimo jars with vulnerability CVE-2011-5034		<a href="#">lists.apache.org</a>
Best 7 Best Internet Security Software in 2019	MISC	<a href="#">www.cnet.com</a>
[karaf-issues] 20210723 [jira] [Created] (KARAF-7227) Upgrade geronimo artifacts to mitigate CVE-2011-5034		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
oCERT.org - oCERT Advisories	MISC	<a href="#">www.ocert.org</a>
[karaf-issues] 20210723 [jira] [Commented] (KARAF-7227) Upgrade geronimo artifacts to mitigate CVE-2011-5034		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>

Pony Mail!	MLIST	<a href="#">lists.a</a>
Pony Mail!	MLIST	<a href="#">lists.a</a>
NEOHAPSIS - Peace of Mind Through Integrity and Insight	BUGTRAQ	<a href="#">archiv</a>
[karaf-issues] 20210723 [jira] [Comment Edited] (KARAF-7227) Upgrade geronimo artifacts to mitigate CVE-2011-5034		<a href="#">lists.a</a>
Pony Mail!	MLIST	<a href="#">lists.a</a>
Pony Mail!	MLIST	<a href="#">lists.a</a>
[geronimo-dev] 20210728 [jira] [Commented] (GERONIMO-6814) Improve Geronimo specs to mitigate CVE-2011-5034		<a href="#">lists.a</a>
[axis-java-dev] 20210622 [jira] [Created] (AXIS2-6004) AXIS 2 1.7.9 geronimo jars with vulnerability CVE-2011-5034		<a href="#">lists.a</a>
VU#903934 - Hash table implementations vulnerable to algorithmic complexity attacks	CERT-VN	<a href="#">www.l</a>
HashCollision-DOS-POC/HashtablePOC.py at master · FireFart/HashCollision-DOS-POC · GitHub	MISC	<a href="#">github</a>
[karaf-issues] 20210726 [jira] [Resolved] (KARAF-7227) Upgrade geronimo artifacts to mitigate CVE-2011-5034		<a href="#">lists.a</a>
Pony Mail!	MLIST	<a href="#">lists.a</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[996908](#) Java (Maven) Security Update for org.apache.geronimo:geronimo (GHSA-v3h8-rw48-h4gr)

© [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](#)