



# CVE-2012-4028

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

## Summary

<b>CVE</b>	CVE-2012-4028
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-07-16 20:55:00 UTC
<b>Updated</b>	2023-03-22 14:10:00 UTC
<b>Description</b>	Tridium Niagara AX Framework does not properly store credential data, which allows context-dependent attackers to bypass

## Risk And Classification

**Problem Types:** CWE-522

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tridium	Niagara Ax	All	All	All	All
Application	Tridium	Niagra Ax Framework	All	All	All	All
Application	Tridium	Niagra Ax Framework	All	All	All	All

## References

Reference	Source	Link
Open Automation Solutions	CONFIRM	<a href="http://www.tridium.com">www.tridium.com</a>
Tridium's Niagara Framework: Marvel of connectivity illustrates new cyber risks - Washington Post	MISC	<a href="http://www.washingtonpost.com">www.washingtonpost.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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](https://status.cve.report)**