



CVE-2012-5353

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

Summary

CVE	CVE-2012-5353
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-09 23:55:05 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Eduserv OpenAthens SP 2.0 for Java allows remote attackers to forge messages and bypass authentication via a SAML as

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:N

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:P/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eduserv	Openathens Service Provider	2.0	-	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References		
Reference	Source	Link
Eduserv - OpenAthens	af854a3a-2127-422b-91ae-364da2661108	status.openathens.org
www.nds.rub.de/media/nds/veroeffentlichungen/2012/08/22/BreakingSAML_3.pdf	af854a3a-2127-422b-91ae-364da2661108	www.nds.rub.de
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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