CVE-2012-0215

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-0215
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-07-12 20:55:09 UTC
Updated	2026-04-29 01:13:23 UTC
Description	model/modelstorage.py in the Tryton application framework (trytond) before 2.4.0 for Python does not properly restrict acce

Risk And Classification

Primary CVSS: v2.0 5.5 from nvd@nist.gov

AV:N/AC:L/Au:S/C:N/I:P/A:P

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:S/C:N/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tryton	Trytond	1.4.13	All	All	All

Application	Tryton	Trytond	1.6.8	All	All	All
Application	Tryton	Trytond	1.8.7	All	All	All
Application	Tryton	Trytond	2.0.5	All	All	All
Application	Tryton	Trytond	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Issue 2476: Missing access control on some relation model for Many2Many - Tryton issue tracker	af854a3a-2127-422b-91ae-364da266110
Tryton: Security Releases for all supported series	af854a3a-2127-422b-91ae-364da266110
Debian -- Security Information -- DSA-2444-1 tryton-server	af854a3a-2127-422b-91ae-364da266110
trytond: 8e64d52ecea4	af854a3a-2127-422b-91ae-364da266110
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

996734 Python (Pip) Security Update for trytond (GHSA-cqg4-rf29-3mv6)