



CVE-2011-2688

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

Summary

CVE	CVE-2011-2688
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-28 18:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-89 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All

Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Mod Authnz External Project	Mod Authnz External	All	All	All	All

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

References						
Reference						
IBM X-Force Exchange						
oss-security - CVE id request: apache mod-auth-external						
Apache 'mod_authnz_external' Module SQL Injection Vulnerability						
Debian update for libapache2-mod-authnz-external - Secunia.com						
Issue 5 - mod-auth-external - Patch for /trunk/mod_authnz_external/mysql/mysql-auth.pl - Apache External Authentication Module - Google Pr						
#633637 - Exploitable remotely: SQL injection - Debian Bug report logs						
oss-security - Re: CVE id request: apache mod-auth-external						
anders.fix.no/software						
Debian -- Security Information -- DSA-2279-1 libapache2-mod-authnz-external						
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.