



CVE-2010-1329

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2010-1329
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-04-15 17:30:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Imperva SecureSphere Web Application Firewall and Database Firewall 5.0.0.5082 through 7.0.0.7078 allow remote attack

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Complete

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Crossbeamsystems	Xos	8.0V5	All	All	All

Operating System	Crossbeamsystems	Xos	8.5.3	All	All	All
Application	Imperva	Securesphere Database Firewall	5.0.0.5082	All	All	All
Application	Imperva	Securesphere Database Firewall	6.0.4.6128	All	All	All
Application	Imperva	Securesphere Database Firewall	6.0.5.6230	All	All	All
Application	Imperva	Securesphere Database Firewall	6.0.5.6238	All	All	All
Application	Imperva	Securesphere Database Firewall	6.0.6.6274	All	All	All
Application	Imperva	Securesphere Database Firewall	6.0.6.6302	All	All	All
Application	Imperva	Securesphere Database Firewall	6.2.0.6442	All	All	All
Application	Imperva	Securesphere Database Firewall	6.2.0.6463	All	All	All
Application	Imperva	Securesphere Database Firewall	7.0.0.7061	All	All	All
Application	Imperva	Securesphere Database Firewall	7.0.0.7078	All	All	All
Application	Imperva	Securesphere Web Application Firewall	5.0.0.5082	All	All	All
Application	Imperva	Securesphere Web Application Firewall	6.0.4.6128	All	All	All
Application	Imperva	Securesphere Web Application Firewall	6.0.5.6230	All	All	All
Application	Imperva	Securesphere Web Application Firewall	6.0.5.6238	All	All	All
Application	Imperva	Securesphere Web Application Firewall	6.0.6.6274	All	All	All
Application	Imperva	Securesphere Web Application Firewall	6.0.6.6302	All	All	All
Application	Imperva	Securesphere Web Application Firewall	6.2.0.6442	All	All	All
Application	Imperva	Securesphere Web Application Firewall	6.2.0.6463	All	All	All
Application	Imperva	Securesphere Web Application Firewall	7.0.0.7061	All	All	All
Application	Imperva	Securesphere Web Application Firewall	7.0.0.7078	All	All	All

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

References						
Reference					Source	
SecurityFocus					af854a3a-2127--	
Imperva SecureSphere Web Application Firewall and Database Firewall Security Bypass Vulnerability					af854a3a-2127--	
CSS10-01: Imperva SecureSphere Web Application Firewall and Database Firewall Bypass Vulnerability (CVE-2010-1329)					af854a3a-2127--	
Imperva - Altogether Better					af854a3a-2127--	
CVE Program record					CVE.ORG	
NVD vulnerability detail					NVD	

No vendor comments have been submitted for this CVE.

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

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)