



CVE-2011-0773

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

Summary

CVE	CVE-2011-0773
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-04 01:00:10 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in pivotx/modules/module_image.php in PivotX before 2.2.3 allows remote attackers

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotx	Pivotx	2.1.0	All	All	All

Application	Pivotx	Pivotx	2.1.1	All	All	All
Application	Pivotx	Pivotx	2.1.2	All	All	All
Application	Pivotx	Pivotx	2.2.0	All	All	All
Application	Pivotx	Pivotx	2.2.0	b1	All	All
Application	Pivotx	Pivotx	2.2.0	b2	All	All
Application	Pivotx	Pivotx	2.2.0	rc	All	All
Application	Pivotx	Pivotx	2.2.1	All	All	All
Application	Pivotx	Pivotx	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

PivotX 2.2.2 Reflected Cross-site Scripting - CXSecurity.com

pivotx on Twitter: "The XSS vulnerability reported today by @packet_storm is fixed in our SVN and PivotX 2.2.3 (with many other fixes) will be

osvdb.org/70672

PivotX 2.2.3 released. - PivotX Blog

PivotX 2.2.2 Cross Site Scripting ≈ Packet Storm

PivotX 2.2.2 Reflected Cross-site Scripting

404 Not Found

PivotX 'module_image.php' Cross Site Scripting Vulnerability

PivotX "image" Cross-Site Scripting Vulnerability - Secunia.com

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.

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