



CVE-2014-7248

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

Summary

CVE	CVE-2014-7248
State	PUBLISHED
Assigner	jpccert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-15 02:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in IPA iLogScanner 4.0 allows remote attackers to inject arbitrary web script or HTM

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	lpa	ilogscanner	4.0	All	All	All

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

References			
Reference	Source		Link
ウェブサイトの攻撃兆候検出ツール iLogScanner : IPA 独立行政法人 情報処理推進機構	af854a3a-2127-422b-91ae-364da2661108		www.
jvndb.jvn.jp/jvndb/JVNDB-2014-000133	af854a3a-2127-422b-91ae-364da2661108		jvndb
JVN#89852154: iLogScanner vulnerable to cross-site scripting	af854a3a-2127-422b-91ae-364da2661108		jvn.jp
CVE Program record	CVE.ORG		www.
NVD vulnerability detail	NVD		nvd.n

No vendor comments have been submitted for this CVE.

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