



CVE-2005-4400

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

Summary

CVE	CVE-2005-4400
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-20 11:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cross-site scripting (XSS) vulnerability in downloads/portal_ent in Liferay Portal Enterprise 3.6.1 and earlier allows remote attackers to execute arbitrary code via a crafted HTTP request.

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: NVD-CWE-Other | 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	Liferay	Liferay Portal Enterprise	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	Link
Liferay Portal Enterprise Multiple Cross-Site Scripting Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securi
Secunia - Advisories - Liferay Portal Enterprise Cross-Site Scripting Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	secunia.cor
- UNSECURED SYSTEMS -: Liferay Portal Enterprise 3.6.1 XSS	af854a3a-2127-422b-91ae-364da2661108	pridels0.blo
www.osvdb.org/21812	af854a3a-2127-422b-91ae-364da2661108	www.osvdb
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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