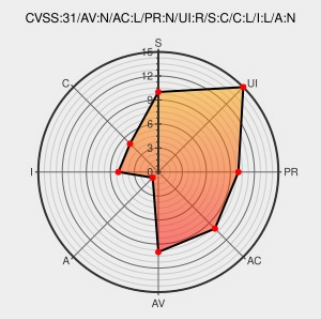
CVE-2011-1133

Published on: 11/05/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1133

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Serendipity from S9y contain the following vulnerability:

Cross-Site Scripting (XSS) in Xinha, as included in the Serendipity package before 1.5.5, allows remote attackers to execute arbitrary code via plugins/ExtendedFileManager/backend.php.

CVE-2011-1133 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
#611661 - Bundled plugins using Xinha allow malicious file uploads - Debian Bug report logs	Third Party Advisory, bugs.debian.org, text/html	DEBIAN 611661
CVE-2011-1133	Third Party Advisory	SECTRACK CVE-2011-1133

	security-tracker.debian.org text/html	
No Description Provided	Release Notes Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM blog.s9y.org/archives/224-Important-Security-Update-Serendipity-1.5.5-released.html
oss-security - Re: CVE requests: freebsd kernel/tesseract/xinha/proftpd	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2011/03/02/5

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	S9y	Serendipity	All	All	All	All
Application	S9y	Serendipity	All	All	All	All

cpe:2.3:a:s9y:serendipity:*:*:*:*:*:*:*:*:

cpe:2.3:a:s9y:serendipity:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→