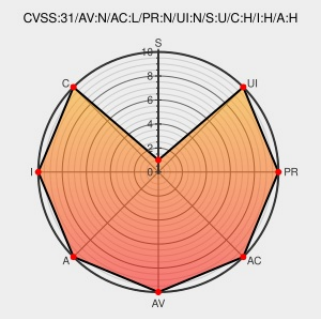
CVE-2011-1134

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

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

CVE-2011-1134

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 in the image manager.

CVE-2011-1134 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
CVE-2011-1134	Third Party Advisory security-tracker.debian.org text/html	SECTRACK CVE-2011-1134
#611661 - Bundled plugins using Xinha allow malicious	Third Party Advisory	DEBIAN 611661

file uploads - Debian Bug report logs	bugs.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→