



CVE-2013-2303

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

Summary

CVE	CVE-2013-2303
State	PUBLISHED
Assigner	jpcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-04-16 14:04:31 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Sleipnir 4.0.0.4000 and earlier on Windows allows remote attackers to spoof the SSL lock icon and address-bar colors via u

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fenrir-inc	Sleipnir	3.9.1.4000	-	All	All

Application	Fenrir-inc	Sleipnir	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	Tags	
jvndb.jvn.jp/jvndb/JVNDB-2013-000032	af854a3a-2127-422b-91ae-364da2661108			jvndb.jvn.jp		
JVN#65034198: Sleipnir for Windows vulnerable to address bar spoofing	af854a3a-2127-422b-91ae-364da2661108			jvn.jp		
CVE Program record	CVE.ORG			www.cve.org	cano	
NVD vulnerability detail	NVD			nvd.nist.gov	cano	
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						