



CVE-2013-7235

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

Summary

CVE	CVE-2013-7235
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-29 14:38:47 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Simple Machines Forum (SMF) before 1.1.19 and 2.x before 2.0.6 allows remote attackers to impersonate arbitrary users v

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simplemachines	Simple Machines Forum	1.0	All	All	All

[illegible]

Application	Simplemachines	Simple Machines Forum	1.1.1	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.10	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.11	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.12	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.13	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.14	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.15	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.16	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.17	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.2	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.3	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.4	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.5	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.6	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.7	All	All	All
Application	Simplemachines	Simple Machines Forum	1.1.8	All	All	All
Application	Simplemachines	Simple Machines Forum	2.0	beta1	All	All
Application	Simplemachines	Simple Machines Forum	2.0	beta2	All	All
Application	Simplemachines	Simple Machines Forum	2.0	beta2.1	All	All
Application	Simplemachines	Simple Machines Forum	2.0	beta3	All	All
Application	Simplemachines	Simple Machines Forum	2.0	beta3.1	All	All
Application	Simplemachines	Simple Machines Forum	2.0	beta4	All	All
Application	Simplemachines	Simple Machines Forum	2.0	rc1	All	All
Application	Simplemachines	Simple Machines Forum	2.0	rc2	All	All
Application	Simplemachines	Simple Machines Forum	2.0	rc3	All	All
Application	Simplemachines	Simple Machines Forum	2.0	rc4	All	All
Application	Simplemachines	Simple Machines Forum	2.0	rc5	All	All
Application	Simplemachines	Simple Machines Forum	2.0.1	All	All	All
Application	Simplemachines	Simple Machines Forum	2.0.2	All	All	All
Application	Simplemachines	Simple Machines Forum	2.0.3	All	All	All
Application	Simplemachines	Simple Machines Forum	2.0.4	All	All	All
Application	Simplemachines	Simple Machines Forum	2.0.5	All	All	All
Application	Simplemachines	Simple Machines Forum	2.0.6	All	All	All
Application	Simplemachines	Simple Machines Forum	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	
oss-security - CVE request: SMF 1.1.19, 2.0.6		af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
oss-security - Re: CVE request: SMF 1.1.19, 2.0.6		af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
Full Disclosure: Multiple vulnerabilities in SMF forum software		af854a3a-2127-422b-91ae-364da2661108	seclists.org	
SMF Downloads		af854a3a-2127-422b-91ae-364da2661108	download.simplemachines.org	
Multiple vulnerabilities in SMF forum software Jakob Lell's Blog		af854a3a-2127-422b-91ae-364da2661108	www.jakoblell.com	
SMF Downloads		MITRE	download.simplemachines.org	
CVE Program record		CVE.ORG	www.cve.org	
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.				