



CVE-2016-1902

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

Summary

CVE	CVE-2016-1902
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-01 22:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The nextBytes function in the SecureRandom class in Symfony before 2.3.37, 2.6.x before 2.6.13, and 2.7.x before 2.7.9 de

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-310 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Sensiolabs	Symfony	2.6.0	All	All	All
Application	Sensiolabs	Symfony	2.6.1	All	All	All
Application	Sensiolabs	Symfony	2.6.10	All	All	All
Application	Sensiolabs	Symfony	2.6.11	All	All	All
Application	Sensiolabs	Symfony	2.6.12	All	All	All
Application	Sensiolabs	Symfony	2.6.2	All	All	All
Application	Sensiolabs	Symfony	2.6.3	All	All	All
Application	Sensiolabs	Symfony	2.6.4	All	All	All
Application	Sensiolabs	Symfony	2.6.5	All	All	All
Application	Sensiolabs	Symfony	2.6.6	All	All	All
Application	Sensiolabs	Symfony	2.6.7	All	All	All
Application	Sensiolabs	Symfony	2.6.8	All	All	All
Application	Sensiolabs	Symfony	2.6.9	All	All	All
Application	Sensiolabs	Symfony	2.7.0	All	All	All
Application	Sensiolabs	Symfony	2.7.1	All	All	All
Application	Sensiolabs	Symfony	2.7.2	All	All	All

Application	Sensiolabs	Symfony	2.7.3	All	All	All
Application	Sensiolabs	Symfony	2.7.4	All	All	All
Application	Sensiolabs	Symfony	2.7.5	All	All	All
Application	Sensiolabs	Symfony	2.7.6	All	All	All
Application	Sensiolabs	Symfony	2.7.7	All	All	All
Application	Sensiolabs	Symfony	2.7.8	All	All	All
Application	Sensiolabs	Symfony	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
CVE-2016-1902: SecureRandom's fallback not secure when OpenSSL fails (Symfony Blog)	af854a3a-2127-422b-91ae-364c
do not ship with a custom rng implementation by fabpot · Pull Request #17359 · symfony/symfony · GitHub	af854a3a-2127-422b-91ae-364c
Debian -- Security Information -- DSA-3588-1 symfony	af854a3a-2127-422b-91ae-364c
CVE-2016-1902: Symfony SecureRandom Lander Brandt	af854a3a-2127-422b-91ae-364c
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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