



CVE-2006-1115

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2006-1115
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-09 13:06:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	nCipher HSM before 2.22.6, when generating a Diffie-Hellman public/private key pair without any specified DiscreteLogGro

Risk And Classification

Primary CVSS: v2.0 2.6 from nvd@nist.gov

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

EPSS: 0.005400000 probability, percentile 0.676490000 (date 2026-04-16)

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Ncipher	Chil	All	All	All	All
Application	Ncipher	Mscapi Csp	5.50	All	All	All
Application	Ncipher	Mscapi Csp	5.54	All	All	All
Application	Ncipher	Ncipher Software Cd	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
IBM X-Force Exchange	af854a3a-2127-42
SecurityFocus	af854a3a-2127-42
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-42
Secunia - Advisories - nCipher Products Multiple Vulnerabilities	af854a3a-2127-42
nCipher Insecure Diffie-Hellman Key Generation Vulnerability	af854a3a-2127-42
nCipher - SA#12: Insecure Generation of Diffie-Hellman keys	af854a3a-2127-42
SecurityTracker.com Archives - nCipher Hardware Security Module May Let Local Users Determine Diffie-Hellman Keys	af854a3a-2127-42
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.