



CVE-2004-2721

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

Summary

CVE	CVE-2004-2721
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The CheckGroup function in openSkat VTMF before 2.1 generates public key pairs in which the "p" variable might not be pr

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Heiko Stamer	Openskat	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
SecurityTracker.com Archives - OpenSkat VTMF CheckGroup() Randomization Error May Let Remote Users Determine Private Keys				af854
OpenSkat Weak Encryption Key Generation Vulnerability				af854
IBM X-Force Exchange				af854
www.osvdb.org/11652				af854
SecureSkat – Freecode				af854
CVE Program record				CVE.0
NVD vulnerability detail				NVD
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				