CVE-2002-0334

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

Summary

CVE	CVE-2002-0334
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-06-25 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	xtell (xtelld) 1.91.1 and earlier, and 2.x before 2.7, allows local users to modify files via a symlink attack on the .xtell-log file.

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:L/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	Xtell	Xtell	1.91.1	All	All	All

Application	Xtell	Xtell	2.6.1	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	Ta
xtell Log File Symbolic Link Attack	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	Pa
Debian -- Security Information -- DSA-121-1 xtell	af854a3a-2127-422b-91ae-364da2661108	www.debian.org	Pa
'Remote exploit against xtelld and other fun' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info	
ISS X-Force Database: xtell-log-symlink (8314): Xtell log symlink	af854a3a-2127-422b-91ae-364da2661108	www.iss.net	Pa
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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