CVE-2002-0332

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

Summary

CVE	CVE-2002-0332
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	Buffer overflows in xtell (xtelld) 1.91.1 and earlier, and 2.x before 2.7, allows remote attackers to execute arbitrary code via

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: NVD-CWE-Other | 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	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
ISS X-Force Database: xtell-bo (8312): Xtell long string buffer overflows	af854a3a-2127-422b-91ae-364da2661108	www.iss.net
Debian -- Security Information -- DSA-121-1 xtell	af854a3a-2127-422b-91ae-364da2661108	www.debian.org
xtell Multiple Remote Buffer Overflow Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.co
'Remote exploit against xtelld and other fun' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
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.