CVE-2002-0134

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

Summary

CVE	CVE-2002-0134
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-03-25 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Telnet proxy in Avirt Gateway Suite 4.2 does not require authentication for connecting to the proxy system itself, which allov

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	Avirt	Avirt Gateway Suite	4.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
'Avirt Gateway Suite Remote SYSTEM Level Compromise' - MARC	af854a3a-212
'Avirt 4.2 question' - MARC	af854a3a-212
ISS X-Force Database: avirt-gateway-telnet-access (7915): Avirt Gateway Suite telnet proxy could allow unauthorized access	af854a3a-212
Avirt Gateway Suite Telnet Proxy Remote SYSTEM Access Vulnerability	af854a3a-212
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.