CVE-2004-1162

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

Summary

CVE	CVE-2004-1162
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-10 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The unison command in scponly before 4.0 does not properly restrict programs that can be run, which could allow remote a

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
Operating System	Gentoo	Linux	All	All	All	All

Application	Scponly	Scponly	2.0	All	All	All
Application	Scponly	Scponly	2.1	All	All	All
Application	Scponly	Scponly	2.3	All	All	All
Application	Scponly	Scponly	2.4	All	All	All
Application	Scponly	Scponly	3.0	All	All	All
Application	Scponly	Scponly	3.11	All	All	All
Application	Scponly	Scponly	3.5	All	All	All
Application	Scponly	Scponly	3.8	All	All	All
Application	Scponly	Scponly	3.9	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
'Re: rssh and scponly arbitrary command execution' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xfor
Gentoo Linux Documentation -- rssh, scponly: Unrestricted command execution	af854a3a-2127-422b-91ae-364da2661108	www.gentoo.o
'rssh and scponly arbitrary command execution' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
scponly homepage	af854a3a-2127-422b-91ae-364da2661108	www.sublimati
SCPOnly Remote Arbitrary Command Execution Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityf
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.