CVE-2009-0367

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

Summary

CVE	CVE-2009-0367
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-05 02:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The Python AI module in Wesnoth 1.4.x and 1.5 before 1.5.11 allows remote attackers to escape the sandbox and execute

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wesnoth	Wesnoth	1.4	All	All	All

Application	Wesnoth	Wesnoth	1.4.1	All	All	All
Application	Wesnoth	Wesnoth	1.4.2	All	All	All
Application	Wesnoth	Wesnoth	1.4.3	All	All	All
Application	Wesnoth	Wesnoth	1.4.4	All	All	All
Application	Wesnoth	Wesnoth	1.4.5	All	All	All
Application	Wesnoth	Wesnoth	1.4.6	All	All	All
Application	Wesnoth	Wesnoth	1.4.7	All	All	All
Application	Wesnoth	Wesnoth	1.5.0	All	All	All
Application	Wesnoth	Wesnoth	1.5.1	All	All	All
Application	Wesnoth	Wesnoth	1.5.10	All	All	All
Application	Wesnoth	Wesnoth	1.5.2	All	All	All
Application	Wesnoth	Wesnoth	1.5.3	All	All	All
Application	Wesnoth	Wesnoth	1.5.4	All	All	All
Application	Wesnoth	Wesnoth	1.5.5	All	All	All
Application	Wesnoth	Wesnoth	1.5.6	All	All	All
Application	Wesnoth	Wesnoth	1.5.7	All	All	All
Application	Wesnoth	Wesnoth	1.5.8	All	All	All
Application	Wesnoth	Wesnoth	1.5.9	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Debian update for wesnoth - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-42
Security advisory for 1.4.x - The Battle for Wesnoth Forums	af854a3a-2127-42
CVE-2009-0367	af854a3a-2127-42
Wesnoth PythonAI Arbitrary Code Execution Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-42
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-42
Debian -- Security Information -- DSA-1737-1 wesnoth	af854a3a-2127-42
404 Not Found	af854a3a-2127-42
Bug #335089 “Please sync wesnoth 1:1.4.7-4 (universe) from Debia...” : Bugs : wesnoth package : Ubuntu	af854a3a-2127-42
Bug #336396 “Wesnoth security fixes” : Bugs : wesnoth package : Ubuntu	af854a3a-2127-42
Battle for Wesnoth - Bugs: bug #13048, Hole in Python AI sandbox permits... [Gna!]	af854a3a-2127-42
packages.debian.org/changelogs/pool/main/w/wesnoth/wesnoth_1.4.7-4/changelog	af854a3a-2127-42
Wesnoth 1.5.11 - The Battle for Wesnoth Forums	af854a3a-2127-42

Wesnoth 1.5.11 - The Battle for Wesnoth Forums	af854a3a-2127-42
IBM X-Force Exchange	af854a3a-2127-42
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.