CVE-2012-2448

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

Summary

CVE	CVE-2012-2448
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-04 16:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	VMware ESXi 3.5 through 5.0 and ESX 3.5 through 4.1 allow remote attackers to execute arbitrary code or cause a denial c

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: CWE-119 | 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	Vmware	Esx	3.5	All	All	All

Operating System	Vmware	Esx	3.5	update1	All	All
Operating System	Vmware	Esx	3.5	update2	All	All
Operating System	Vmware	Esx	3.5	update3	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	4.1	All	All	All
Operating System	Vmware	Esxi	3.5	All	All	All
Operating System	Vmware	Esxi	3.5	1	All	All
Operating System	Vmware	Esxi	4.0	All	All	All
Operating System	Vmware	Esxi	4.0	1	All	All
Operating System	Vmware	Esxi	4.0	2	All	All
Operating System	Vmware	Esxi	4.0	3	All	All
Operating System	Vmware	Esxi	4.0	4	All	All
Operating System	Vmware	Esxi	4.1	All	All	All
Operating System	Vmware	Esxi	4.1	1	All	All
Operating System	Vmware	Esxi	4.1	2	All	All
Operating System	Vmware	Esxi	5.0	All	All	All

Vendor Declared Affected Products

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

References

Reference
osvdb.org/81693
VMSA-2012-0009.2
VMware ESX NFS Traffic Remote Code Execution Vulnerability
VMware ESX/ESXi NFS Flaw Lets Remote Users Execute Arbitrary Code and RPC Pointer Errors Let Local Users Gain Elevated Privileges -
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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