



CVE-2012-1516

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-1516
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-04 16:55:00 UTC
Updated	2019-09-27 18:13:00 UTC
Description	The VMX process in VMware ESXi 3.5 through 4.1 and ESX 3.5 through 4.1 does not properly handle RPC commands, wh

Risk And Classification

Problem Types: CWE-119

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	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	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

References

Reference

IBM X-Force Exchange

VMware ESX/ESXi NFS Flaw Lets Remote Users Execute Arbitrary Code and RPC Pointer Errors Let Local Users Gain Elevated Privileges - VMSA-2012-0009.2

Repository / Oval Repository

VMware Multiple Products Multiple Memory Corruption Privilege Escalation Vulnerabilities

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.