



CVE-2012-1515

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

Summary

CVE	CVE-2012-1515
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-02 10:46:00 UTC
Updated	2018-10-12 22:02:00 UTC
Description	VMware ESXi 3.5, 4.0, and 4.1 and ESX 3.5, 4.0, and 4.1 do not properly implement port-based I/O operations, which allow

Risk And Classification

Problem Types: CWE-264

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	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	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	4.0	All	All	All
Operating System	Vmware	Esxi	4.1	All	All	All
Operating System	Vmware	Esxi	3.5	All	All	All
Operating System	Vmware	Esxi	4.0	All	All	All
Operating System	Vmware	Esxi	4.1	All	All	All

References

Reference	Source	Link
Microsoft Security Bulletin MS12-042 - Important Microsoft Docs	MS	docs.microsoft.com
US-CERT Alert TA12-164A -- Microsoft Updates for Multiple Vulnerabilities	CERT	www.us-cert.gov

Repository / Oval Repository	OVAL	oval.cisecurity.org
Microsoft Windows and VMware ESXi/ESX CVE-2012-1515 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com/bid/50840
VMSA-2012-0006.2	CONFIRM	www.vmware.com/security/vmsa-2012-0006.2
Repository / Oval Repository	OVAL	oval.cisecurity.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com/vulnerabilities/50840
VMware ESXi and ESX ROM Overwrite Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTrack	www.securitytracker.com/id?1036444
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.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report