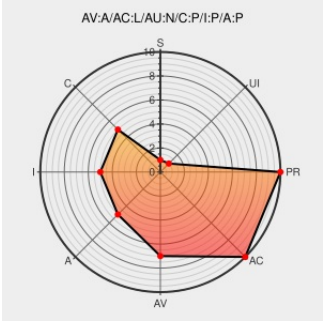
# CVE-2014-3793

Published on: 05/31/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

## CVE-2014-3793

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Esxi from Vmware contain the following vulnerability:

VMware Tools in VMware Workstation 10.x before 10.0.2, VMware Player 6.x before 6.0.2, VMware Fusion 6.x before 6.0.3, and VMware ESXi 5.0 through 5.5, when a Windows 8.1 guest OS is used, allows guest OS users to gain guest OS privileges or cause a denial of service (kernel NULL pointer dereference and guest OS crash) via unspecified vectors.

CVE-2014-3793 has been assigned by cve@mitre.org to track the vulnerability

## CVSS2 Score: 5.8 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| ADJACENT_NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

## CVE References

| Description | Tags | Link |
|---|---|---|
| VMware ESXi VMware Tools Bug Lets Local Users Gain Elevated Privileges - SecurityTracker | www.securitytracker.com text/html | SECTRACK 1030311 |
| VMSA-2014-0005 \| United States | www.vmware.com text/html | CONFIRM www.vmware.com/security/advisories/VMSA-2014-0005.html |
| VMware Security Advisory 2014-0005 ≈ Packet Storm | packetstormsecurity.com text/html | MISC packetstormsecurity.com/files/126869/VMware-Security-Advisory-2014-0005.html |
| SecurityFocus | www.securityfocus.com text/html | BUGTRAQ 20140530 NEW VMSA-2014-0005 - VMware Workstation, Player, Fusion, and ESXi patches address a guest privilege escalation |

| | | |
|---|---|---|
| Security Advisory SA58894 - VMware Multiple Products Windows Guest Privilege Escalation Vulnerability - Secunia | web.archive.org text/html | SECUNIA 58894 |
| VMware Workstation/Player/Fusion VMware Tools Bug Lets Local Users Gain Elevated Privileges - SecurityTracker | www.securitytracker.com text/html | SECTRACK 1030310 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Vmware | Esxi | 5.0 | All | All | All |
| Operating System | Vmware | Esxi | 5.0 | 1 | All | All |
| Operating System | Vmware | Esxi | 5.0 | 2 | All | All |
| Operating System | Vmware | Esxi | 5.1 | All | All | All |
| Operating System | Vmware | Esxi | 5.1 | 1 | All | All |
| Operating System | Vmware | Esxi | 5.5 | All | All | All |
| Operating System | Vmware | Esxi | 5.0 | All | All | All |
| Operating System | Vmware | Esxi | 5.0 | 1 | All | All |
| Operating System | Vmware | Esxi | 5.0 | 2 | All | All |
| Operating System | Vmware | Esxi | 5.1 | All | All | All |
| Operating System | Vmware | Esxi | 5.1 | 1 | All | All |
| Operating System | Vmware | Esxi | 5.5 | All | All | All |
| Application | Vmware | Fusion | 6.0 | All | All | All |
| Application | Vmware | Fusion | 6.0.1 | All | All | All |
| Application | Vmware | Fusion | 6.0.2 | All | All | All |
| Application | Vmware | Fusion | 6.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Vmware | Fusion | 6.0.1 | All | All | All |
| Application | Vmware | Fusion | 6.0.2 | All | All | All |
| Application | Vmware | Player | 6.0 | All | All | All |
| Application | Vmware | Player | 6.0.1 | All | All | All |
| Application | Vmware | Player | 6.0 | All | All | All |
| Application | Vmware | Player | 6.0.1 | All | All | All |
| Application | Vmware | Workstation | 10.0 | All | All | All |
| Application | Vmware | Workstation | 10.0.1 | All | All | All |
| Application | Vmware | Workstation | 10.0 | All | All | All |
| Application | Vmware | Workstation | 10.0.1 | All | All | All |

cpe:2.3:o:vmware:esxi:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.0:1:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.0:2:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.1:1:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.5:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.0:1:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.0:2:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.1:1:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.5:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:player:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:player:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:player:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:player:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation:10.0:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation:10.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation:10.0:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation:10.0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
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 registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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