



# CVE-2017-4903

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-4903
<b>State</b>	PUBLIC
<b>Assigner</b>	security@vmware.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-06-07 18:29:00 UTC
<b>Updated</b>	2022-02-03 19:43:00 UTC
<b>Description</b>	VMware ESXi 6.5 without patch ESXi650-201703410-SG, 6.0 U3 without patch ESXi600-201703401-SG, 6.0 U2 without patch

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)


Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	-	All	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	5.5	All	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	5.5	-	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	5.5	1	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	5.5	2	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	5.5	3a	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	5.5	3b	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	All	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	-	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	1	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	1a	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	1b	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	2	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	3	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	3a	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	600-201504401	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esxi</a>	6.0	600-201505401	All	All

Operating System	Vmware	Esxi	6.0	600-201507101	All	All
Operating System	Vmware	Esxi	6.0	600-201507102	All	All
Operating System	Vmware	Esxi	6.0	600-201507401	All	All
Operating System	Vmware	Esxi	6.0	600-201507402	All	All
Operating System	Vmware	Esxi	6.0	600-201507403	All	All
Operating System	Vmware	Esxi	6.0	600-201507404	All	All
Operating System	Vmware	Esxi	6.0	600-201507405	All	All
Operating System	Vmware	Esxi	6.0	600-201507406	All	All
Operating System	Vmware	Esxi	6.0	600-201507407	All	All
Operating System	Vmware	Esxi	6.0	600-201509101	All	All
Operating System	Vmware	Esxi	6.0	600-201509102	All	All
Operating System	Vmware	Esxi	6.0	600-201509201	All	All
Operating System	Vmware	Esxi	6.0	600-201509202	All	All
Operating System	Vmware	Esxi	6.0	600-201509203	All	All
Operating System	Vmware	Esxi	6.0	600-201509204	All	All
Operating System	Vmware	Esxi	6.0	600-201509205	All	All
Operating System	Vmware	Esxi	6.0	600-201509206	All	All
Operating System	Vmware	Esxi	6.0	600-201509207	All	All
Operating System	Vmware	Esxi	6.0	600-201509208	All	All
Operating System	Vmware	Esxi	6.0	600-201509209	All	All
Operating System	Vmware	Esxi	6.0	600-201509210	All	All
Operating System	Vmware	Esxi	6.0	600-201510401	All	All
Operating System	Vmware	Esxi	6.0	600-201511401	All	All
Operating System	Vmware	Esxi	6.0	600-201601101	All	All
Operating System	Vmware	Esxi	6.0	600-201601102	All	All
Operating System	Vmware	Esxi	6.0	600-201601401	All	All
Operating System	Vmware	Esxi	6.0	600-201601402	All	All
Operating System	Vmware	Esxi	6.0	600-201601403	All	All
Operating System	Vmware	Esxi	6.0	600-201601404	All	All
Operating System	Vmware	Esxi	6.0	600-201601405	All	All
Operating System	Vmware	Esxi	6.0	600-201602401	All	All
Operating System	Vmware	Esxi	6.0	600-201603101	All	All
Operating System	Vmware	Esxi	6.0	600-201603102	All	All
Operating System	Vmware	Esxi	6.0	600-201603201	All	All
Operating System	Vmware	Esxi	6.0	600-201603202	All	All

Operating System	Vmware	Esxi	6.0	600-201603203	All	All
Operating System	Vmware	Esxi	6.0	600-201603204	All	All
Operating System	Vmware	Esxi	6.0	600-201603205	All	All
Operating System	Vmware	Esxi	6.0	600-201603206	All	All
Operating System	Vmware	Esxi	6.0	600-201603207	All	All
Operating System	Vmware	Esxi	6.0	600-201603208	All	All
Operating System	Vmware	Esxi	6.0	600-201605401	All	All
Operating System	Vmware	Esxi	6.0	600-201608101	All	All
Operating System	Vmware	Esxi	6.0	600-201608401	All	All
Operating System	Vmware	Esxi	6.0	600-201608402	All	All
Operating System	Vmware	Esxi	6.0	600-201608403	All	All
Operating System	Vmware	Esxi	6.0	600-201608404	All	All
Operating System	Vmware	Esxi	6.0	600-201608405	All	All
Operating System	Vmware	Esxi	6.0	600-201610410	All	All
Operating System	Vmware	Esxi	6.0	600-201611401	All	All
Operating System	Vmware	Esxi	6.0	600-201611402	All	All
Operating System	Vmware	Esxi	6.0	600-201611403	All	All
Operating System	Vmware	Esxi	6.0	600-201702101	All	All
Operating System	Vmware	Esxi	6.0	600-201702102	All	All
Operating System	Vmware	Esxi	6.0	600-201702201	All	All
Operating System	Vmware	Esxi	6.0	600-201702202	All	All
Operating System	Vmware	Esxi	6.0	600-201702203	All	All
Operating System	Vmware	Esxi	6.0	600-201702204	All	All
Operating System	Vmware	Esxi	6.0	600-201702205	All	All
Operating System	Vmware	Esxi	6.0	600-201702206	All	All
Operating System	Vmware	Esxi	6.0	600-201702207	All	All
Operating System	Vmware	Esxi	6.0	600-201702208	All	All
Operating System	Vmware	Esxi	6.0	600-201702209	All	All
Operating System	Vmware	Esxi	6.0	600-201702210	All	All
Operating System	Vmware	Esxi	6.0	600-201702211	All	All
Operating System	Vmware	Esxi	6.0	600-201702212	All	All
Operating System	Vmware	Esxi	6.0	u1	All	All
Operating System	Vmware	Esxi	6.0	u2	All	All
Operating System	Vmware	Esxi	6.0	u3	All	All
Operating System	Vmware	Esxi	6.5	All	All	All

Operating System	Vmware	Esxi	6.5	-	All	All
Operating System	Vmware	Esxi	6.5	650-201701001	All	All
Operating System	Vmware	Esxi	6.5	650-201703001	All	All
Operating System	Vmware	Esxi	6.5	650-201703002	All	All
Operating System	Vmware	Esxi	5.5	All	All	All
Operating System	Vmware	Esxi	6.0	All	All	All
Operating System	Vmware	Esxi	6.0	u1	All	All
Operating System	Vmware	Esxi	6.0	u2	All	All
Operating System	Vmware	Esxi	6.0	u3	All	All
Operating System	Vmware	Esxi	6.5	All	All	All
Application	Vmware	Fusion	All	All	All	All
Application	Vmware	Fusion	8.0.0	All	All	All
Application	Vmware	Fusion	8.0.1	All	All	All
Application	Vmware	Fusion	8.0.2	All	All	All
Application	Vmware	Fusion	8.1.0	All	All	All
Application	Vmware	Fusion	8.1.1	All	All	All
Application	Vmware	Fusion	8.5.0	All	All	All
Application	Vmware	Fusion	8.5.1	All	All	All
Application	Vmware	Fusion	8.5.2	All	All	All
Application	Vmware	Fusion	8.5.3	All	All	All
Application	Vmware	Fusion	8.5.4	All	All	All
Application	Vmware	Fusion	8.5.5	All	All	All
Application	Vmware	Fusion	8.0.0	All	All	All
Application	Vmware	Fusion	8.0.1	All	All	All
Application	Vmware	Fusion	8.0.2	All	All	All
Application	Vmware	Fusion	8.1.0	All	All	All
Application	Vmware	Fusion	8.1.1	All	All	All
Application	Vmware	Fusion	8.5.0	All	All	All
Application	Vmware	Fusion	8.5.1	All	All	All
Application	Vmware	Fusion	8.5.2	All	All	All
Application	Vmware	Fusion	8.5.3	All	All	All
Application	Vmware	Fusion	8.5.4	All	All	All
Application	Vmware	Fusion	8.5.5	All	All	All
Application	Vmware	Fusion Pro	All	All	All	All
Application	Vmware	Workstation Player	All	All	All	All
Application	Vmware	Workstation Player	12.0.0	All	All	All



Application	VMware	Workstation Pro	12.5.4	All	All	All
<b>References</b>						
<b>Reference</b>						
VMSA-2017-0006						
VMware ESXi Buffer Overflow and Memory Initialization Errors Let Local Guest System Users Obtain Potentially Sensitive Information and Ex						
VMware Workstation/Fusion Buffer Overflow and Memory Initialization Errors Let Local Guest System Users Obtain Potentially Sensitive Infor						
Multiple VMware Products CVE-2017-4903 Local Memory Corruption Vulnerability						
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.						

© [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](#) 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](#)