



CVE-2007-0063

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

Summary

CVE	CVE-2007-0063
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-21 19:17:00 UTC
Updated	2019-07-16 12:20:00 UTC
Description	Integer underflow in the DHCP server in EMC VMware Workstation before 5.5.5 Build 56455 and 6.x before 6.0.1 Build 550

Risk And Classification

Problem Types: CWE-191

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Application	Vmware	Ace	All	All	All	All
Application	Vmware	Ace	All	All	All	All
Operating System	Vmware	Esx	2.0.2	All	All	All
Operating System	Vmware	Esx	2.1.3	All	All	All
Operating System	Vmware	Esx	2.5.3	All	All	All
Operating System	Vmware	Esx	2.5.4	All	All	All
Operating System	Vmware	Esx	3.0.0	All	All	All
Operating System	Vmware	Esx	3.0.1	All	All	All
Operating System	Vmware	Esx	2.0.2	All	All	All
Operating System	Vmware	Esx	2.1.3	All	All	All
Operating System	Vmware	Esx	2.5.3	All	All	All

Operating System	Vmware	Esx	2.5.4	All	All	All
Operating System	Vmware	Esx	3.0.0	All	All	All
Operating System	Vmware	Esx	3.0.1	All	All	All
Application	Vmware	Player	All	All	All	All
Application	Vmware	Player	All	All	All	All
Application	Vmware	Server	All	All	All	All
Application	Vmware	Server	All	All	All	All
Application	Vmware	Workstation	All	All	All	All
Application	Vmware	Workstation	All	All	All	All

References

Reference	Source	Link	Ta
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	Th
VMware Workstation 6 Release Notes	CONFIRM	www.vmware.com	Pa
VMware Player Release Notes	CONFIRM	www.vmware.com	Pa
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Th
USN-543-1: VMWare vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Th
[Full-Disclosure] Mailing List Charter	FULLDISC	lists.grok.org.uk	Th
VMware Server Release Notes	CONFIRM	www.vmware.com	Pa
VMware DHCP Bugs Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytracker.com	Th
Gentoo Linux Documentation -- VMware Workstation and Player: Multiple vulnerabilities	GENTOO	security.gentoo.org	Th
VMware Workstation DHCP Server Multiple Remote Code Execution Vulnerabilities	BID	www.securityfocus.com	Pa
Gentoo update for vmware - Advisories - Secunia	SECUNIA	secunia.com	Th
VMWare Products Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com	Th
VMware Workstation 5.5 Release Notes	CONFIRM	www.vmware.com	Pa
VMware ACE Release Notes	CONFIRM	www.vmware.com	Pa
VMware Player Release Notes	CONFIRM	www.vmware.com	Pa
VMware ACE Release Notes	CONFIRM	www.vmware.com	Pa
VMWare DHCP Server Remote Code Execution Vulnerabilities	ISS	www.iss.net	Pa
Ubuntu update for vmware - Advisories - Secunia	SECUNIA	secunia.com	Th
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Organization	Published	Contributor	Statement
--------------	-----------	-------------	-----------

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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

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