



CVE-2005-4459

Published on: 12/21/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

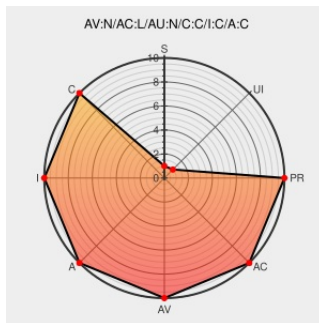
CVE-2005-4459

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Ace](#) from [Vmware](#) contain the following vulnerability:

Heap-based buffer overflow in the NAT networking components vmnat.exe and vmnet-natd in VMWare Workstation 5.5, GSX Server 3.2, ACE 1.0.1, and Player 1.0 allows remote authenticated attackers, including guests, to execute arbitrary code via crafted (1) EPRT and (2) PORT FTP commands.

CVE-2005-4459 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
VMWare Remote Arbitrary Code Execution Vulnerability	Patch cve.report (archive) text/html	🌐 BID 15998
[Full-disclosure] [ACSSEC-2005-11-25-0x1] VMWare Workstation 5.5.0 <= build-18007 G SX Server Variants And Others	Exploit web.archive.org text/html Inactive Link Not Archived	🌐 FULLDISC 20051221 [ACSSEC-2005-11-25-0x1] VMWare Workstation 5.5.0 <= build-18007 G SX Server Variants And Others
Gentoo Linux Documentation -- VMware Workstation: Vulnerability in NAT networking	www.gentoo.org text/html	🌐 GENTOO GLSA-200601-04
VMware Knowledge Base - Answer	Patch web.archive.org text/html	vmw CONFIRM www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=2000

Inactive Link Not Archived

SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20051221 [Security-Advisories (at) acs-inc (dot) com [email concealed]: [Full-disclosure] [ACSSEC-2005-11-25-0x1] VMWare Workstation 5.5.0 <= build-18007 G SX Server Variants And Others]
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20051221 VMware vulnerability in NAT networking
Secunia - Advisories - Gentoo update for vmware	Vendor Advisory web.archive.org text/html	 SECUNIA 18344
Webmail OVH- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2005-3013
SecurityReason - VMWare Workstation 5.5.0 <= build-18007 G SX Server Variants And Others	securityreason.com text/html	 SREASON 282
SecurityTracker.com Archives - VMware Flaw in NAT Function Lets Remote Users Execute Arbitrary Code	securitytracker.com text/html	 SECTRAK 1015401
SecurityReason - VMware vulnerability in NAT networking	securityreason.com text/html	 SREASON 289
US-CERT Vulnerability Note VU#856689	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#856689
Secunia - Advisories - VMware NAT Networking Buffer Overflow Vulnerability	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 18162

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
Application	Vmware	Ace	1.0	All	All	All
Application	Vmware	Ace	1.0	All	All	All
Application	Vmware	Gsx Server	2.0	All	All	All
Application	Vmware	Gsx Server	2.0.1_build_2129	All	All	All
Application	Vmware	Gsx Server	2.5.1	All	All	All
Application	Vmware	Gsx Server	2.5.1_build_5336	All	All	All
Application	Vmware	Gsx Server	2.5.2	All	All	All
Application	Vmware	Gsx Server	3.0	All	All	All

Application	Vmware	Gsx Server	3.0_build_7592	All	All	All
Application	Vmware	Gsx Server	3.1	All	All	All
Application	Vmware	Gsx Server	3.2	All	All	All
Application	Vmware	Gsx Server	2.0	All	All	All
Application	Vmware	Gsx Server	2.0.1_build_2129	All	All	All
Application	Vmware	Gsx Server	2.5.1	All	All	All
Application	Vmware	Gsx Server	2.5.1_build_5336	All	All	All
Application	Vmware	Gsx Server	2.5.2	All	All	All
Application	Vmware	Gsx Server	3.0	All	All	All
Application	Vmware	Gsx Server	3.0_build_7592	All	All	All
Application	Vmware	Gsx Server	3.1	All	All	All
Application	Vmware	Gsx Server	3.2	All	All	All
Application	Vmware	Player	1.0.0	All	All	All
Application	Vmware	Player	1.0.0	All	All	All
Application	Vmware	Workstation	3.2.1	patch1	All	All
Application	Vmware	Workstation	3.4	All	All	All
Application	Vmware	Workstation	4.0	All	All	All
Application	Vmware	Workstation	4.0.1	All	All	All
Application	Vmware	Workstation	4.0.2	All	All	All
Application	Vmware	Workstation	4.5.2	All	All	All
Application	Vmware	Workstation	4.5.2_build_8848	r4	All	All
Application	Vmware	Workstation	5.0.0_build_13124	All	All	All
Application	Vmware	Workstation	5.5	All	All	All
Application	Vmware	Workstation	3.2.1	patch1	All	All
Application	Vmware	Workstation	3.4	All	All	All
Application	Vmware	Workstation	4.0	All	All	All
Application	Vmware	Workstation	4.0.1	All	All	All
Application	Vmware	Workstation	4.0.2	All	All	All
Application	Vmware	Workstation	4.5.2	All	All	All
Application	Vmware	Workstation	4.5.2_build_8848	r4	All	All
Application	Vmware	Workstation	5.0.0_build_13124	All	All	All
Application	Vmware	Workstation	5.5	All	All	All
cpe:2.3:a:vmware:ace:1.0:*****:						
cpe:2.3:a:vmware:ace:1.0:*****:						
cpe:2.3:a:vmware:gsx_server:2.0:*****:						

```
cpe:2.3:a:vmware:gsx_server:2.0.1_build_2129:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:vmware:gsx_server:2.5.1:::~::~:
```

```
cpe:2.3:a:vmware:gsx_server:2.5.1_build_5336:::*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:2.5.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:3.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:3.0_build_7592:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:3.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:3.2:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:2.0:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:2.0.1:build 2129:*.:.:.:.:.:
```

```
cpe:2.3:a:vmware:gsx_server:2.5.1:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:vmware:gsx_server:2.5.1_build_5336:*.:.:*.:.:.*
```

```
cpe:2.3:a:vmware:gsx_server:2.5.2:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:3.0:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:3.0 build 7592:*:*:*:*.*.*
```

```
cpe:2.3:a:vmware:gsx_server:3.1.*:*:*:*:*:
```

```
cpe:2.3:a:vmware:gsx_server:3.2:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:player:1.0.0:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:player:1.0.0:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation:3.2.1:patch1:::*:*.*.*.*.*
```

```
cpe:2.3:a:vmware:workstation:3.4:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation:4.0:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation:4.0.1:::*:*:*.*
```

```
cpe:2.3:a:vmware:workstation:4.0.2:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation:4.5.2:*:*:*:*:*:
```

```
cpe:2.3:a:vmware:workstation:4.5.2_build_8848:r4:*.:.:.:.:
```

```
cpe:2.3:a:vmware:workstation:5.0.0_build_13124.*:*:*:*:*.*.*
```

```
cpe:2.3:a:vmware:workstation:5.5:*:*:*:*:*:
```

cpe:2.3:a:vmware:workstation:3.2.1:patch1:*****:
cpe:2.3:a:vmware:workstation:3.4:*****:
cpe:2.3:a:vmware:workstation:4.0:*****:
cpe:2.3:a:vmware:workstation:4.0.1:*****:
cpe:2.3:a:vmware:workstation:4.0.2:*****:
cpe:2.3:a:vmware:workstation:4.5.2:*****:
cpe:2.3:a:vmware:workstation:4.5.2_build_8848:r4:*****:
cpe:2.3:a:vmware:workstation:5.0.0_build_13124:*****:
cpe:2.3:a:vmware:workstation:5.5:*****:

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 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](#)