Security Research Advisory

VMware vCenter Update Manager
Multiple Vulnerabilities

Table of Contents

SUMMARY 3

PATH TRAVERSAL 4

VULNERABILITY DETAILS 4
TECHNICAL DETAILS 4

MULTIPLE CROSS-SITE SCRIPTING (XSS) 5

VULNERABILITY DETAILS 5
TECHNICAL DETAILS 5

LEGAL NOTICES 6

Summary

VMware vCenter Update Manager is an automated patch management solution for VMware ESX hosts and Microsoft virtual machines.

The installation of VMware vCenter Update Manager includes an outdated, unpatched version of the Jetty web server. Multiple vulnerabilities affecting this version were publicly disclosed, including CERT402580 (JETTY-1004), CVE-2009-1524 and CVE-2007-6672. Through these vulnerabilities, an unauthenticated attacker can access arbitrary files on the system running vCenter Update Manager (usually the same running the vCenter Server) or execute Cross Site Scripting attacks.

Date	Details
21/05/2010	Vendor disclosure
28/05/2010	Vendor acknowledgment
19/07/2010	Patch release
16/11/2010	Public disclosure

Path Traversal

Path Traversal					Advisory Number
					SN-10-03
Severity	Software	Version	Accessibility	CVE	Author(s)
H	VMware vCenter Update Manager	4.0.0.3971	Remote	*n/a*	Claudio Criscione
	Vendor URL		Advisory URL		
	http://www.vmware.com		-		

Vulnerability Details

Access to the file system can be achieved through a path traversal vulnerability under the credentials of the user running the Update Manager – usually Local System.

By leveraging this vulnerability a skilled attacker can compromise the vCenter Server, accessing default files storing critical authentication data.

Further details can be found in the original Jetty advisories.

Technical Details

Description

Attackers can exploit this vulnerability with any HTTP capable tool. Vasto Beta 0.2 includes a Metasploit module to exploit the issue.

The following URL is provided as a Proof of Concept.

```
http://ServerIP:9084/vci/downloads/health.xml/%3F/../../../../../../../../../boot.ini
```

Multiple Cross-Site Scripting (XSS)

Multiple Cross-Site Scripting (XSS)					Advisory Number
					SN-10-03
Severity	Software	Version	Accessibility	CVE	Author(s)
M	VMware vCenter Update Manager	4.0.0.3971	Remote	*n/a*	Claudio Criscione
	Vendor URL		Advisory URL		
	http://www.vmware.com		-		

Vulnerability Details

Cross Site Scripting attacks can be performed on any directory with Directory Listing enabled. A potential attacker could easily craft malicious link in order to inject arbitrary javascript code and compromise victim's browser.

Further details can be found in the original Jetty advisories.

Technical Details

Description

The following URL will trigger a basic XSS attack.

```
http://ServerIP:9084/vum-fileupload/;%3Cscript%3Ealert('XSS%20on%20Update')%3C/script%3E
```

Legal Notices

Secure Network (*www.securenetwork.it*) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.