
# Security Research Advisory

## VMware Studio 2

## Path Traversal Vulnerability

# Table of Contents

<table>
<tr><td colspan="5">Path Traversal</td><td>Advisory Number<br>SN-09-03</td></tr>
<tr><td>Severity</td><td>Software</td><td>Version(s)</td><td>Accessibility</td><td>CVE</td><td>Author(s)</td></tr>
<tr><td rowspan="3">H</td><td>VMware Studio</td><td>2.0.0.946-172280</td><td>Remote</td><td>-</td><td rowspan="3">Claudio Criscione</td></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">http://www.vmware.com</td><td colspan="2">-</td></tr>
</table>

| Date | Details |
|---|---|
| 06/07/2009 | Vendor disclosure |
| 06/07/2009 | Vendor acknowledgment |
| 01/09/2009 | Patch release |
| 09/09/2009 | Public disclosure |

# Summary

VMware Studio provides mechanisms for authoring, on-site management, distributing and deployment of production-ready virtual appliances.

An arbitrary file upload vulnerability, due to a path traversal in a file upload script, has been identified.

# Vulnerability Details

Due to an improper sanitization of user' input, a support component of VMware Studio's web interface can be tricked into uploading a file to any directory (according to the web server's user permission), failing to remove the file afterwards. The issue was fixed in the final release of VMware 2.0

# Technical Details

## Description

An attacker can trivially upload any file on the server, possibly in the /opt/vmware/share/htdocs directory, where any python file will be executed, resulting in arbitrary code execution on the server.

In order to trigger the path traversal, filename has to be prepended by the usual "*../*" string.

## Vulnerable Code

File: *service/depot/upload-tar.py*

```
data = item.file.read()
[..]
temp_dir = tempfile.mkdtemp()
f = open(temp_dir + "/" + item.filename, 'w')
f.write(data)
```

The script will accept any form providing a file named "servicetar", writing its content on the file system, as can be seen above.

# 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.



| | |
|---|---|
| **e-mail** | info@securenetwork.it |
| **phone** | +39 02 917 730 41 |