

# [NEWS] Adobe Version Cue VCNative Multiple Vulnerabilities (Privileges Escalation, Symlink Attack)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0105.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 08/30/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 30 Aug 2005 18:10:16 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----  
Adobe Version Cue VCNative Multiple Vulnerabilities (Privileges Escalation, Symlink Attack)

## SUMMARY

" <<http://www.adobe.com/products/creativesuite/versioncue.html>> Adobe Version Cue is a software version tracking system for Adobe products distributed with Adobe Creative Suite and select Adobe products."

Lack of proper parameter checking and random name supplying allow attackers to gain root privileges and perform a symlink attack using Adobe Version Cue VCNative.

## DETAILS

### Vulnerable Systems:

- \* Adobe Version Cue version 1 on the Apple OS X platform

### Privileges Escalation:

Local exploitation of a design error in Adobe's Version Cue allows local attackers to gain root privileges. Version Cue includes a setuid root application named VCNative which contains a design error that allows local

## Securiteam: [NEWS] Adobe Version Cue VCNative Multiple Vulnerabilities (Privileges Escalation, Symlink Attack)

attackers to gain root privileges. The vulnerability specifically exists due to an unchecked command line option parameter.

The "-lib" command line option allows users to specify library "bundles" which allows for the introduction of arbitrary code in the context of a root owned process. The init function in a shared library is executed immediately upon loading. By utilizing the "-lib" argument to load a malicious library, local attackers can execute arbitrary code with root privileges.

Successful exploitation allows local attackers to write to arbitrary files with user-supplied data. Data written to the linked file will include some corrupted data as well as user-supplied data, potentially corrupting a file completely and preventing the execution of system commands. In addition, a carefully crafted input value can be used in conjunction with standard system tools such as cron to gain root privileges.

### Symlink Attack:

Local exploitation of a design error in Adobe Systems, Inc. Version Cue allows local attackers to gain root privileges. Version Cue includes a setuid root application named VCNative which is vulnerable to a symlink attack. The vulnerability specifically exists due to the use of predictable log file names. VCNative uses a format such as "VCNative-[pid].log" for the filename and stores the file in the current working directory. Attackers can easily predict the created filename and supply user-controlled data via the "-host" and "-port" options. A carefully supplied value can cause a crafted "log file" to be written. Crafted strings written to root-owned files can lead to arbitrary code execution with root privileges.

Successful exploitation allows local attackers to write to arbitrary files with user-supplied data. Data written to the linked file will include some corrupted data as well as user-supplied data, potentially corrupting a file completely and preventing the execution of system commands. In addition, a carefully crafted input value can be used in conjunction with standard system tools such as cron to gain root privileges.

### Workaround:

Remove the setuid bit from the VCNative binary and execute the application as a root.

### Vendor Status:

The vendor has issued a fix for the vulnerabilities. For more information see: <<http://www.adobe.com/support/downloads/detail.jsp?ftpID=2985>>  
<http://www.adobe.com/support/downloads/detail.jsp?ftpID=2985>

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1842>>  
CAN-2005-1842  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1843>>  
CAN-2005-1843

Securiteam: [NEWS] Adobe Version Cue VCNative Multiple Vulnerabilities (Privileges Escalation, Symlink Attack)

Disclosure Timeline:

06/27/2005 Initial vendor notification

06/27/2005 Initial vendor response

08/29/2005 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<mailto:idlabs-advisories@lists.idefense.com> iDEFENSE Labs.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=296&type=vulnerabilities>>

<http://www.idefense.com/application/poi/display?id=296&type=vulnerabilities>,

<<http://www.idefense.com/application/poi/display?id=297&type=vulnerabilities>>

<http://www.idefense.com/application/poi/display?id=297&type=vulnerabilities>

The vendor advisory can be found at:

<<http://www.adobe.com/support/techdocs/327129.html>>

<http://www.adobe.com/support/techdocs/327129.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.