



July 26, 2006

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2006-07-28

Apache 1.3.29/2.X mod_rewrite Buffer Overflow Vulnerability

CVE-2006-3747

- **Synopsis**

Mod_rewrite is an Apache module that can be used to remap requests based on regular expression matches of the requested URI. A buffer overflow vulnerability exists when dealing with rewritten URI's that are prefixed with the LDAP protocol scheme.

Exploitation leads to remote access to the vulnerable machine and therefore the risk factor is critical.

- **Vulnerable Systems**

Apache 1.3.29/mod_rewrite
Apache 2.0.x/mod_rewrite - only 2.0.46 and higher are vulnerable
Apache 2.2.x/mod_rewrite

- **Vulnerability Information**

The mod_rewrite module contains an off-by-one buffer overflow vulnerability when escaping an absolute URI scheme. The vulnerability occurs within `escape_absolute_uri()` when separating out tokens within an LDAP URL. Triggering the vulnerability results in a pointer to user-controlled data to be written outside of the bounds of a character pointer array, which in many cases can be used to gain complete control of the affected host.

Note that an LDAP-specific rule does not need to exist to exploit the vulnerability. However, a rule must exist with the following properties:

- A rule must exist where the user can control the initial part of the rewritten URL
 - The rule must not contain a forbidden or gone flag [F or G]
 - Rules with "noescape" [NE] flag settings are not affected.
-

- **Resolution**

Apache has posted an update:

<http://www.apache.org/dist/httpd/Announcement2.2.html>

- **Credits**

This vulnerability was discovered by Mark Dowd of McAfee Avert Labs.

- **Legal Notice**

Copyright (C) 2006 McAfee, Inc.

The information contained within this advisory is provided for the convenience of McAfee's customers, and may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way. McAfee makes no representations or warranties regarding the accuracy of the information referenced in this document, or the suitability of that information for your purposes.

McAfee, Inc. and McAfee Avert Labs are registered Trademarks of McAfee, Inc. and/or its affiliated companies in the United States and/or other Countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.
