

NISCC Vulnerability Advisory 821765/NISCC/Apache

Vulnerability Issues with Apache HTTPD

Version Information

Advisory Reference	821765/NISCC/Apache
Release Date	27 July 2006
Last Revision	27 July 2006
Version Number	1.0

Acknowledgement

This vulnerability was reported to NISCC by the Apache Security Team.

What is Affected?

The following products are affected:

- Apache HTTPD v1.3 from v1.3.28
- Apache HTTPD v2.0 from v2.0.46
- Apache HTTPD v2.2 from v2.2.0

Impact

If exploited, this vulnerability could allow arbitrary code to be executed remotely.

Severity

High

Summary

The Apache HTTP Server is a free software/open source web server for Unix-like systems, Microsoft Windows, Novell NetWare and other platforms.

In July 2006, the Apache Security Team was contacted by McAfee Avert Labs, regarding an 'off-by-one' error that could lead to remote code execution.

The Apache Software Foundation is aware of this vulnerability and has produced patches to address the problem. Please see 'Solution' for details on patches required to address this flaw.

Details

CVE ID: CVE-2006-3747

The issue is an 'off-by-one' error in the LDAP scheme handling of `mod_rewrite`. For some RewriteRules, this could lead to a pointer being written out of bounds.

Please note that the flaw does not affect a default installation of the Apache HTTP Server.

Exploitation of this issue is reliant on all of the following factors:

1. Vulnerable versions of Apache as outlined above (in the 'What is affected?' section). Earlier versions of Apache HTTPD are not vulnerable.
2. The server has `mod_rewrite` configured and enabled in the configuration (directive "RewriteEngine on").

Please note that this is not a normal default configuration.

3. A rewrite rule where the remote user can influence the beginning of a rewritten URL. For example, the following rule is vulnerable:

```
RewriteRule fred/(.*) $1
```

But this rule is not:

```
RewriteRule fred/(.*) joe/$1
```

4. The stack frame layout - the stack frame layout varies depending on the operating system (OS), the architecture, the compiler, the compiler options, the Apache version and so on.

Solution

Patches are available from the Apache Software Foundation. Please visit their website for further details (<http://www.apache.org/>).

Also please refer to the 'Vendor Information' section of this advisory for platform specific remediation.

Vendor Information

The following vendors have provided information about how their products are affected by this vulnerability.

Fedora Project

Juniper Networks

Red Hat, Inc

Fedora Project

Vendor statement: Fedora Project

Vulnerable

The ability to exploit this issue is dependent on the stack layout for a particular compiled version of mod_rewrite. The Fedora Project has analyzed Fedora Core 4 and 5 binaries and determined that these distributions are vulnerable to this issue. However this flaw does not affect a default installation of Fedora Core; users who do not use, or have not enabled, the Rewrite module are not affected by this issue.

Updates to correct this issue are available, see <http://fedora.redhat.com/Download/updates.html>

Juniper

Juniper Networks products are not susceptible to this vulnerability.

Red Hat, Inc

Vendor statement: Red Hat, Inc

Not vulnerable

This issue does not affect the version of Apache HTTPD as supplied with Red Hat Enterprise Linux 2.1.

The ability to exploit this issue is dependent on the stack layout for a particular compiled version of mod_rewrite. If the compiler has added padding to the stack immediately after the buffer being overwritten, this issue can not be exploited, and Apache HTTPD will continue operating normally.

The Red Hat Security Response Team analyzed Red Hat Enterprise Linux 3 and Red Hat Enterprise Linux 4 binaries for all architectures as shipped by Red Hat and determined that these versions cannot be exploited. We therefore do not plan on providing updates for this issue.

For technical details see: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=200219

Credits

The NISCC Vulnerability Management Team would like to thank the Apache Security Team for reporting this issue to NISCC.

The NISCC Vulnerability Management Team would also like to thank the vendors for their co-operation in the handling of this vulnerability.

Contact Information

The NISCC Vulnerability Management Team can be contacted as follows:

Email	vulteam@nisc.gov.uk <i>(Please quote the advisory reference in the subject line.)</i>
Telephone	+44 (0)870 487 0748 Extension 4511 <i>(Monday to Friday 08:30 -17:00)</i>
Fax	+44 (0)870 487 0749
Post	Vulnerability Management Team NISCC PO Box 832 London SW1P 1BG

We encourage those who wish to communicate via email to make use of our PGP key. This is available from <http://www.nisc.gov.uk/nisc/publicKey2-en.pop>.

Please note that UK government protectively marked material should not be sent to the email address above.

If you wish to be added to our email distribution list, please email your request to uniras@nisc.gov.uk.

What is NISCC?

For further information regarding the UK National Infrastructure Security Co-Ordination Centre, please visit the NISCC web site at: <http://www.nisc.gov.uk/>

Reference to any specific commercial product, process or service by trade name, trademark manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favouring

by NISCC. The views and opinions of authors expressed within this notice shall not be used for advertising or product endorsement purposes.

Neither shall NISCC accept responsibility for any errors or omissions contained within this advisory. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

© 2006 Crown Copyright

Revision History

27 July 2006 Initial release (1.0)

<End of NISCC Vulnerability Advisory>