

[VulnWatch] NSFOCUS SA2006-03 : IBM AIX rm_mlcache_file Local Race Condition Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-04/msg00013.html>

- *From:* NSFOCUS Security Team <security@xxxxxxxxxxx>
 - *Date:* Mon, 24 Apr 2006 16:37:05 +0800
-

NSFOCUS Security Advisory (SA2006-03)

IBM AIX rm_mlcache_file Local Race Condition Vulnerability

Release Date: 2006-04-24

CVE ID: CVE-2006-1247

<http://www.nsfocus.com/english/homepage/research/0603.htm>

Affected systems & software

=====

IBM AIX 5.1

IBM AIX 5.2

IBM AIX 5.3

Unaffected systems & software

=====

Summary

=====

NSFocus Security Team discovered a local race condition in IBM AIX rm_mlcache_file which could allow a local user to overwrite arbitrary file.

Description

=====

rm_mlcache_file shipped with IBM AIX is used to delete some cached files. By default it is set with suid root bit.

rm_mlcache_file contains a race condition when processing temporary files which allows a local attacker to overwrite arbitrary files. Attackers can launch attacks by running the program directly, or waiting till root user runs it. Successful exploitation may result in data loss or DoS, specifically depending on the overwritten file.

Workaround

=====

Remove the execution bit from rm_mlcache_file temporarily:

```
# chmod 000 /usr/bin/rm_mlcache_file
```

Vendor Status

=====

The vendor has released the following APAR patches to fix the vulnerability:

APAR number for AIX 5.1.0: IY82866

APAR number for AIX 5.2.0: IY82285

APAR number for AIX 5.3.0: IY82357

AIX 5 APAR patch can be downloaded at:

<http://www.ibm.com/servers/eserver/support/unixservers/aixfixes.html>

The temporary patch for the vulnerability can be downloaded at:

ftp://aix.software.ibm.com/aix/efixes/security/rm_mlcache_file_ifix.tar.Z

Additional Information

=====

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2006-1247 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems. Candidates may change significantly before they become official CVE entries.

Acknowledgment

=====

Yang Jilong of NSFocus Security Team found the vulnerability.

DISCLAIMS

=====

THE INFORMATION PROVIDED IS RELEASED BY NSFOCUS "AS IS" WITHOUT WARRANTY OF ANY KIND. NSFOCUS DISCLAIMS ALL WARRANTIES, EITHER EXPRESSED OR IMPLIED, EXCEPT FOR THE WARRANTIES OF MERCHANTABILITY. IN NO EVENT SHALL NSFOCUS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF NSFOCUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. DISTRIBUTION OR REPRODUCTION OF THE INFORMATION IS PROVIDED THAT THE ADVISORY IS NOT MODIFIED IN ANY WAY.

Copyright 1999-2006 NSFOCUS. All Rights Reserved. Terms of use.

NSFOCUS Security Team <security@xxxxxxxxxxx>

[VulnWatch] NSFOCUS SA2006-03 : IBM AIX rm_mlcache_file Local Race Condition Vulnerability

NSFOCUS INFORMATION TECHNOLOGY CO.,LTD

(<http://www.nsfocus.com>)

PGP Key: <http://www.nsfocus.com/homepage/research/pgpkey.asc>

Key fingerprint = F8F2 F5D1 EF74 E08C 02FE 1B90 D7BF 7877 C6A6 F6DA

Attachment: pgpDJabEW5Zcb.pgp

Description: PGP signature