

[UNIX] LSF eauth Vulnerability Leads to Remote Code Execution (LSF_From_PC)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0083.html>

From: SecuriTeam (*support_at_securiteam.com*)
Date: 02/26/04

To: list@securiteam.com
Date: 26 Feb 2004 12:02:00 +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>

LSF eauth Vulnerability Leads to Remote Code Execution (LSF_From_PC)

SUMMARY

"eauth" is the component within <http://www.platform.com> LSF (Load Sharing Facility) which controls authentication. Specific input data strings can be constructed and can cause failure of the eauth binary, leading to the code execution under root privileges. This security risk is contained to "local cluster". This means that it can be exploited remotely (from one host to another) but only between hosts within the LSF cluster.

DETAILS

Vulnerable Systems:

- * Load Sharing Facility versions 4.x, 5.x, 6.x

Tests shows, that it is possible to cause SIGSEGV on eauth. The bug is in 'eauth -s' mode.

This is how you can reproduce the bug:

```
$ eauth -s ??????????????????????????????????????[press Enter]
1006 1006 eKlempa 192.168.10.106 4110 20 user ? [press Enter]
LSF_From_PC AAAAAAAAAAAAAAAAAAAAAAAAAA ??????????[press Enter]
```

Securiteam: [UNIX] LSF eauth Vulnerability Leads to Remote Code Execution (LSF_From_PC)

Segmentation fault (core dumped)

This bug is exploitable (i.e. attacker can change program execution flow and point it to code of her choice, effectively gaining root access privilege). As everyone can execute 'eauth' and it is setuid==root, attacker can locally gain root privileges by exploiting it. Moreover, while 'eauth -s' is used by daemons like 'mbatchd' to authorize clients, it is possible to exploit this vulnerability on remote host within a cluster.

How to patch:

This problem has been directly addressed in a security patch released for LSF. The fix is contained to the "eauth" binary which will need to be replaced for each platform used in the cluster. The patch can be downloaded from Platform FTP site.

FTP: ftp.platform.com

Path: patches/<version>/os/<os>/eauth*

Example: patches/5.1/os/sparc-sol7-64/eauth5.1_sparc-sol7-64.Z

If the OS or version is not currently available, it can be built on demand. Please contact Platform Technical Support if you have any questions or concerns. Phone: 1-877-444-4573 or Email: support@platform.com

References:

This bug was confirmed in Platform's official security advisory dated 9 Feb 2004. It is accessible directly from Platform as Knowledge Base Article KB1-5RZ11.

ADDITIONAL INFORMATION

The information has been provided by <mailto:cadence@aci.com.pl> Tomasz Grabowski.

=====

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.