

# [NEWS] Mathematica License Manager Hostname Spoofing

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0031.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/03/01

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Subject: [NEWS] Mathematica License Manager Hostname Spoofing

Message-Id: <20010803114500.CB3CD13902@mail.der-keiler.de>

Date: Fri, 3 Aug 2001 13:45:00 +0200 (CEST)

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

## Mathematica License Manager Hostname Spoofing

---

### SUMMARY

Mathematica License Manager can be tricked into returning a valid license when it should not. This is caused by the fact that the License Manager trusts whatever the clients sends it (the clients sends the License Manager its hostname and user ID). This would enable an attacker to steal a valid license key and to cause a denial of service attack ("license starvations").

### DETAILS

Vulnerable systems:

Mathematica version 4.0

Mathematica version 4.1

The Mathematica license manager resides on a license server, and listens to requests for licenses from mathematica programs running on other machines on the net (we'll call them clients). The way it works is that the client sends it's hostname and the uid of the user that mathematica is running as (or 65536 in the case of a Windows machine) to mathlm on the server, and it is up to mathlm to grant a license or not. By default mathlm will grant a license to everyone who asks but it does come with an option, "--restrict anyprogramyouwant", that will run a program of your choice, and depending on it's output, grant or refuse to grant a license to the requesting client. More specifically, if your restrict program returns a 1 to mathlm, a license is granted, otherwise a license is

Hypermail Development List: [NEWS] Mathematica License Manager

denied.

This seems like a great idea, having the ability to restrict access to mma licenses with any program you like (and write), but the problem is that the mathematica client can be trivially tricked into sending any information you want to the license manager. For example, the hostname of the machine mma is running on, this means that any restricting program that bases its decision on what the client tells it (e.g. the requesting client's hostname) can be tricked into granting a license when one really should not be granted.

This could also be used in a denial of service attack, since the spoofing machine could simply request all of the available licenses from the server.

Workaround:

Use a firewall or some form of packet filtering, and drop packets destined to port 16286 from unknown hosts.

ADDITIONAL INFORMATION

The information has been provided by <mailto:pinwheel@shout.net>  
Pinwheel.

=====

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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.



- *Next message:* [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] Linksys EtherFast Security Vulnerability (Username and Password Disclosure)"
- *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[TOOL] SSH Secure Shell 3.0.0 Vulnerability Scanner"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)