

Securiteam: [NEWS] Intuity Audix Voicemail Restricted Interface Circumvention (rexec)

[NEWS] Intuity Audix Voicemail Restricted Interface Circumvention (rexec)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0022.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/12/03

To: list@securiteam.com

Date: 12 May 2003 17:16:54 +0200

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

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Intuity Audix Voicemail Restricted Interface Circumvention (rexec)

SUMMARY

<<http://www.avaya.com/>> Avaya, a manufacturer of telecommunications products, makes a voicemail system called Intuity Audix. A vulnerability in the product allows remote attacker to access the operating system in an unrestricted manner.

DETAILS

This vulnerability is not truly a 100% remote shell vulnerability, due to the fact that the user must either know the "sa" user password, or is able to sniff the network that the Intuity Audix machine is on. This will also work with the "vm" user, or any other user who wishes to authenticate over the network via telnet.

The Avaya ASA GUI-based administrator uses port 23 as the default means of authentication. Therefore, using a simple network analyzer one can obtain a username and password.

Securiteam: [NEWS] Intuity Audix Voicemail Restricted Interface Circumvention (rexec)

By using 'rexec' and issuing the following command, we can gain access the account without any restrictions:

```
rexec <ip address> -l(username) move /mtce/login/(username)/.profile  
/mtce/login/(username)/.profile2
```

For example:

```
rexec 192.168.0.1 -lsa move /mtce/login/sa/.profile  
/mtce/login/sa/.profile2
```

ADDITIONAL INFORMATION

The information has been provided by Cushman.

=====

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.