

[NEWS] Axis Network Camera Requires No Authentication to Access Sensitive Information

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0061.html>

From: support@securiteam.com

Date: 12/15/01

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 15 Dec 2001 13:48:45 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Axis Network Camera Requires No Authentication to Access Sensitive Information

SUMMARY

Axis Network Cameras suffers from a security flaw in the CGI they include. The vulnerability is that the CGIs are accessible without any requirement for authentication even though they reveal a lot of sensitive information.

DETAILS

Vulnerable systems:

Axis Network Cameras firmware 2.0x

Immune systems:

Axis Network Cameras firmware 2.12 and above

The Axis Network Cameras contain two CGIs /cgi-bin/paramtool and /cgi-bin/hwtestio, accessing them requires no authorization of any kind. This seems to be a mis-configuration of the web server.

Paramtool can be used like this:

<http://>/cgi-bin/paramtool?--blargh>

This will show the entire configure of the webcam, including:

Securiteam: [NEWS] Axis Network Camera Requires No Authentication to Access Sensitive Information

root.InternalSecurity.Passwd { root { passwd ["plAsx1.0CzA.wd"] (...)

This could also reveal dialup info, like phone-numbers, username, and passwords (If this camera is set up to be serving images through dialup connection).

Then there is also /cgi-bin/hwtestio, which is really a bad thing to allow access to.

The CGI will allow you to restart the Camera as many times as you want ("for testing proposes of course).

Example:

You can do "<http://>/cgi-bin/hwtestio?-r242424>", and the camera restarts.

Solution:

Upgrading to the latest firmware solves both these issues.

ADDITIONAL INFORMATION

The information has been provided by <mailto:trenger@trenger.ro> Torgeir Hansen.

=====

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.

-
- **Previous message:** support@securiteam.com: "[\[TOOL\] LDAP Authentication Brute Forcing](#)"
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)