

[NEWS] FlexWATCH Authorization Bypassing and XSS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0087.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/26/04

To: list@securiteam.com

Date: 26 Feb 2004 14:06:53 +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>

FlexWATCH Authorization Bypassing and XSS Vulnerability

SUMMARY

<<http://www.flexwatch.com/>> FlexWATCH Network Camera and video server series are "all stand-alone video transmission system to deliver crystal clear real time live video over the TCP/IP network. FlexWATCH System has a built-in web server that enable you to view live video through standard web browser such as MSIE or Netscape Navigator".

FlexWATCH is vulnerable to two security vulnerabilities, one allows bypassing the authentication mechanism, the other allows causing a cross site scripting vulnerability.

DETAILS

Vulnerable Systems:

* FlexWATCH-Webs version 2.2

Authorization Bypassing:

By supplying an additional '/' at the begining of the URLs sent to the server, an attacker can bypass the authorization requirement on certain pages.

