Vulnerability Report

Lund, Sweden Oct 29, 2014

VU#680244 – CERT XSS vulnerability

Overview:

Source: CERT- Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page."

Vulnerable products, firmware and applications:

Axis video products with firmware version prior to 5.50 are vulnerable.

Impact on Axis products, systems and users:

The vulnerability is located on the live view page of the product which can be accessed by anyone including administrators. Specific scripts could then be crafted to virtually modify anything in the targeted product.

Axis plan:

The XSS vulnerability has been addressed and is shipping with products' firmware 5.50 and above.

For products running earlier revisions, Service will be made available on request.