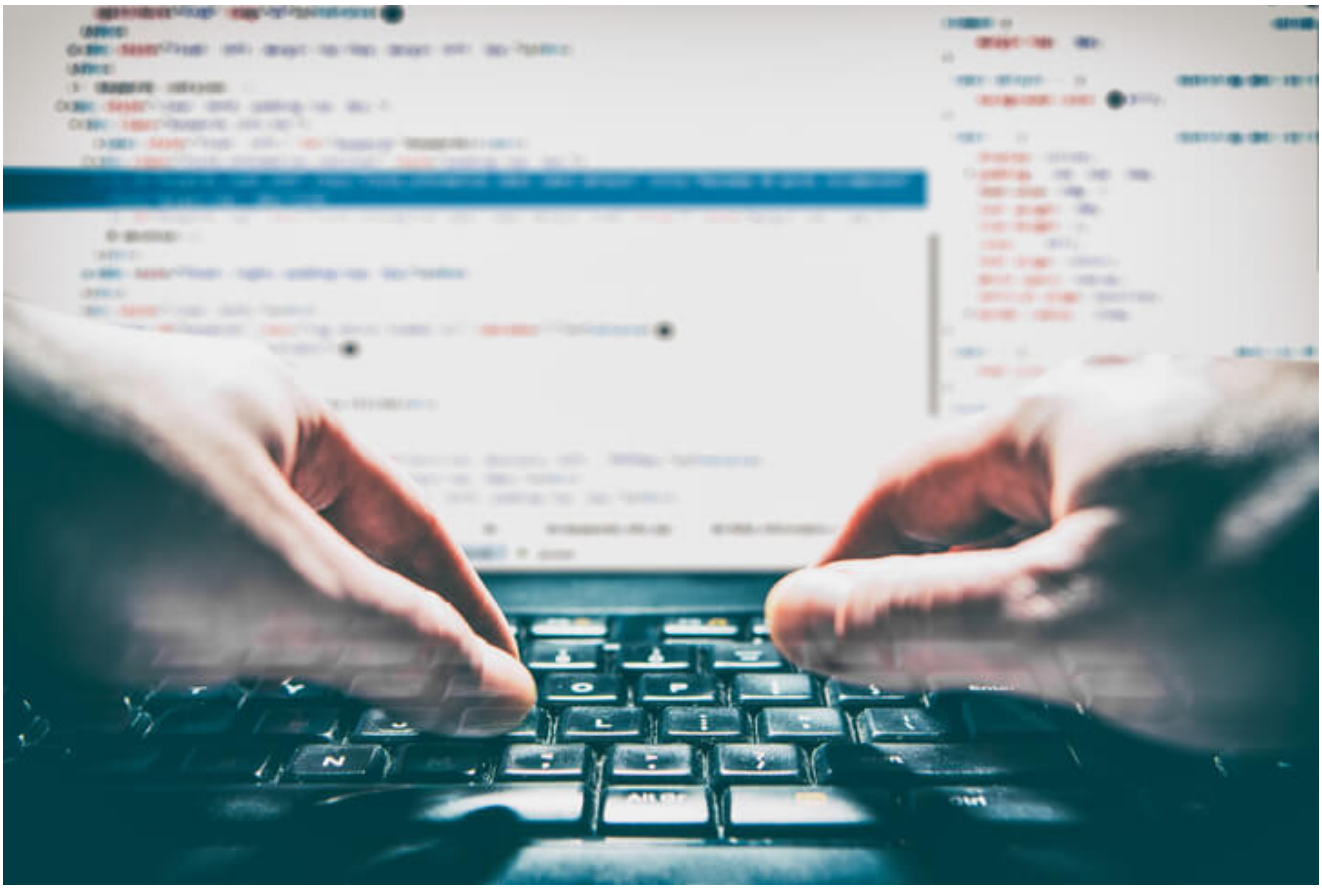
Stored XSS Vulnerabilites on Foscam

fortinet.com/blog/threat-research/stored-xss-vulnerabilites-on-foscam-3

March 31, 2016



In case you missed it, Fortinet recently introduced the Fortinet Network Security Academy (FNSA) with the objective of providing individuals with advanced cybersecurity skills in order to address the industry's current skills shortage.

To highlight the value of such a program, the team at our French offices regularly collaborate with students who work with us on a range of security projects. The following discovery is the product of one such student collaboration project.

Summary

After successfully gaining access to the File System on an IP Camera via a serial connection, as recorded in a previous post, the plan was to explore the File System for potential vulnerabilities.

To do this, Fortinet, in collaboration with Eurecom, organized a student project. During the investigation, Emanuele Cozzi of Eurecom found a flaw in the IP camera's file system UI (more specifically, in the CGI scripts). The discovered flaw allows an attacker to inject code

into certain pages, and to even upload an exploited version of its firmware with a back door enabled onto the vulnerable camera.

Proof of Concept

The flaw exists in two CGI scripts on the camera that allow injection of code, one with a limit of 20 characters, and the other allowing 64 characters (except ', \, \n, \r) to be injected.

While a 20 character limit isn't very useful as an exploit opportunity, 64 characters is large enough to allow the injection of something more effective onto the camera. The following video demonstrates an attack scenario where a phishing page is injected using one of the discovered vulnerabilities

A typical attack scenario for phishing a camera's login credentials would involve an HTTP request of the form:

http: //[IP]/[VULNERABLE_SCRIPT].cgi?host=

<[INJECTED_HTML]>&next_url=index.htm&cam_user=[USERNAME]&cam_pwd=[PASSWORD]

In the video, the flawed CGI script is exploited to make it point to an attacker's phishing URL that resembles the Foscam Web UI Login page. Through this phishing page, an attacker could upload backdoored firmware versions to the camera.

Exploitation

Prerequisites for an Attack

Knowledge of an authorized username and password on the IP Camera.

Although, this doesn't sound like an obvious piece of information to have, a *significant* number of cameras connected to the internet make use of commonlyknown default credentials.

Conditions under which an Attack would work

- Cameras using the default username and password that all new cameras come configured with are especially vulnerable. This is particularly damaging for cameras with UI 2.4.10.5 or 2.4.10.10.
- To avoid the problem of default credentials, the latest Foscam Web UI (Version 2.4.10.12) requires a user to change the camera's username and password upon first login. However, these cameras are vulnerable to the above XSS vulnerabilities until that first login.

Foscam maintains that their cameras are secure due to the following reasons :

- The attacker must already know the login username and password.
- On the latest version of the UI, a mandatory username/password change is required upon first login, preventing the possibility of cameras accessible with default credentials. As an added layer of security, there are restrictions based on the strength of the new password.

Special thanks to Aurelien Francillon of Eurecom and to Axelle Apvrille.