Vulnerability Report

Lund, Sweden August 12, 2016

CVE-2016-AXIS-0812 Remote Format String

Overview:

An independent researcher has discovered and disclosed a critical vulnerability in the Server-Side Include Daemon (SSID) present in the firmware of certain Axis products. By exploiting a format string log function using specially crafted byte sequences, it is possible for an attacker to gain root access to a product without authentication.

The exploit is in the form of an executable python script and was made publicly available by the researcher on July 18th, 2016. Service releases have been developed for affected products and partners and customers has been informed prior to the disclosure.

External sources:

The Python script was disclosed by the researcher on July 18th, 2016 to several well-known exploit sites:

https://www.exploit-db.com/
http://seclists.org/bugtraq/

Affected products and firmware:

AXIS Network Cameras firmware versions between 5.20 and to 6.20.
AXIS Network Door Controllers firmware versions before 1.45.0
AXIS Network Video Door Stations firmware versions before 5.85.1.2
AXIS Network I/O Relay Modules firmware versions before 1.00.0.1
AXIS Network Horn Speakers firmware versions before 1.20.2

Impact on systems and users:

An attacker needs to have network access to products in order to exploit the vulnerability. Affected Axis devices that are exposed directly to the Internet are at immediate risk. This includes products that are behind a router/firewall where port-forwarding/UPnP NAT traversal has been enabled.

Root access to an Axis product provides the attacker with complete system access and the potential for them to add new users, disrupt the service of the product and in some cases even take over the product.

Devices that are behind a protected network are at low risk. Network cameras connected to AVHS (AXIS Video Hosting System) are at low risk. Network cameras part of AXIS Camera

Companion solution are at low risk, as the remote connection solution does not expose cameras to direct Internet access.

Axis recommendations:

Axis strongly recommends to upgrade products at high risk immediately. Axis recommends to upgrade low-risk products in a scheduled manner.

Service Releases:

Service Releases which patch the vulnerability in SSID have been built for all affected products. The list of available service releases can be found at
http://origin-www.axis.com/ftp/pub_soft/MPQT/SR/service-releases.txt

The firmware images can be downloaded directly from
ftp://ftp.axis.com/pub_soft/MPQT/ for Axis video products and
ftp://ftp.axis.com/pub_soft/PACS/ for Axis Door Controller, Speaker and Relay products.