*Lund, Sweden July 5, 2016*

# CVE-2016-AXIS-0705 Remote Format String

**Overview:**

An independent researcher discovered a critical vulnerability that makes it possible for an attacker to gain root access to certain Axis products without authentication. The exploit is very advanced and the researcher intends to publish full disclosure on July 18th, 2016.

**External sources:**

The external disclosure is due July 18th
*Note: This CVE will be updated once the exploit is disclosed.*

**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.
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. Axis recommends to upgrade products in low risk in a scheduled and controlled manner.

**Service Release:**

List of available service releases can be found at
http://origin-www.axis.com/ftp/pub_soft/MPQT/SR/service-releases.txt