

Lund, Sweden Oct 26, 2014

CVE-2014-3566 SSL/Poodle

Overview:

Source: US-CERT/NIST <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566>

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security over networks. HTTPS is the standard HTTP network protocol in combination with a secure SSL/TLS channel.

POODLE is a weakness in the SSL 3.0 protocol. An attacker can exploit it to recover small amounts of plaintext from an encrypted SSL 3.0 connection, by issuing crafted HTTPS requests, for example created by client-side Javascript code. Multiple HTTPS requests are required for each recovered plaintext byte, and the vulnerability allows attackers to confirm if a particular byte was guessed correctly. This vulnerability is inherent to SSL 3.0 and unavoidable in this protocol version. The fix is to upgrade to the TLS protocol.

Vulnerable products, firmware and applications:

Axis products support SSLv3 and are affected by the vulnerability.

Impact on Axis products, systems and users:

This vulnerability is only applicable to products configured to use HTTPS. Products installed on critical systems that are configured to only allow HTTPS connects need immediate attention. Risk level is low if the camera is only accessible within a LAN for a malicious client to exploit the vulnerability. Risk level is high if the products are accessible from the internet.

Axis recommendations:

SSLv3 should be disabled for products installed in critical environments where clients are required to use HTTPS to gain access. Some old clients may not support the TLS protocol and will not be able to make HTTPS connection to the product.

Please contact Axis support (<http://www.axis.com/techsup/index.htm>) for instructions how to disable SSLv3.

Axis plan:

Axis is planning to ship products and firmware that have disabled SSLv3 by default.

Cameras/Encoders: Firmware 5.70.

Access control: Firmware 1.25.0.

Please follow Axis recommendations until these firmwares are available.

Axis Communications AB, Emdalavägen 14, SE-223 69 Lund, Sweden.

Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com,

Vat.No. SE 556253-614301