Vulnerability Report

Lund, Sweden Jan 30, 2015

CVE-2015-0235 Ghost - gethostbyname

Overview:

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0235

The vulnerability allows a malicious service to append a 4 or 8 byte buffer overflow data when calling the glibc function gethostbyname(). The 4/8 bytes may be written into memory and possibly executed if it contains binary code for the platform it executes on.

Vulnerable products, firmware and applications:

Axis products firmware includes the Linux glibc which includes this vulnerability.

Impact on systems and users:

This vulnerability cannot be exploited by an external malicious client. The gethostbyname() function is used by internal camera services when accessing external internet resources. Typically camera actions such as http notification, sending email or NTP. It is not possible to configure these services to make a buffer overflow call to gethostbyname(). We have not been able to exploit the vulnerability in our internal tests but cannot yet guarantee that it is not possible. An attacker would require camera administrator access privileges.

Axis recommendations:

The practical exposure risk is extremely low. Protect the cameras with good and unique password.

Axis plan:

Axis follows the Linux community vulnerability patches. Future firmware versions for our products will include an updated glibc which patches this vulnerability.

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