Vulnerability Report

Lund, Sweden Mar 09, 2016

CVE-2015-7547: glibc getaddrinfo

Overview:

Source: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7547

Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.

Vulnerable products, firmware and applications:

Axis camera firmware from 2008 includes the vulnerable glibc package and thus affected by the vulnerability.

Impact on systems and users:

It is possible to exploit the product vulnerability if the DNS server has been compromised or redirected with a man-in-the-middle attack vulnerability. The cameras also need to use services such as NTP, FTP or SMTP and the URL to the network services needs to be configured with domain names.

Axis recommendations:

Red Hat list a number of ways to mitigate

```
- A local resolver (that drops non-compliant responses)
- A firewall that drops UDP DNS packets > 512 bytes.
```

It is also possible to configure the services in the camera to use fix IP-address instead of host.domain names. If NTP, FTP or SMTP is not used at all you may disable the DNS-server under Setup | System Options | Network | TCP/IP | Advanced.

Axis plan:

Axis will roll out camera firmware with the patched glibc library in Q2 2016.

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