Security Advisory

November 2017

CVE-2016-2147 / 48 (udhcpc/busybox)

Source:

- CVE-2016-2147
  Integer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to cause a denial of service (crash) via a malformed RFC1035-encoded domain name, which triggers an out-of-bounds heap write.
- CVE-2016-2148
  Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to have unspecified impact via vectors involving OPTION_6RD parsing.

Overview

BusyBox is a common open source package found in many embedded Linux devices. If there is an acting DHCP server on the local network which is compromised with malicious code, it is possible to crash the BusyBox DHCP client on affected network devices. It is potentially possible for a skilled adversary to develop an exploit that executes arbitrary code on these devices.

Risk assessment

The risk of a malicious DHCP server present on the local network depends on the protection, processes and policies for the network. There are no known exploits that target Axis devices specifically. A crashed BusyBox DHCP client will automatically be restarted.

Risk mitigation

As a precaution, customers are advised to update to the latest version (see below) and ensure control over all the DHCP severs on the local network. Axis devices using static IP addresses (not DHCP) are not at risk.

Patched Firmware and Models

Patched firmware for affected products is available for download at https://www.axis.com/support/firmware. The release notes for the patched firmware will state "Corrected security vulnerability CVE-2016-2147/48"

You may also use AXIS Camera Management (https://www.axis.com/products/axis-camera-management) that will help fetching and installing the latest firmware to Axis products in your system.

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

Affected Models:

A1001, A8004, A8105-E, A9161, A9188, A9188-VE, ACB-LE, ACC-L, ACC-LW, ACD-V, ACD-WV, ACE-L, ACR, C1004-E, C2005, C3003, F34, F41, F44, F44 Dual Audio Input, M1004-W, M1011, M1011-W, M1013, M1014, M1025, M1031-W, M1033-W, M1034-W, M1045-LW, M1054, M1065-L, M1065-LW, M1103, M1104, M1113, M1114, M1124, M1125, M1143-L, M1144-L, M1145, M1145-L, M2014-E, P1204, P1214, P1214-E, P1224-E, P12_M20, P8524, M2025-LE, M2026-LE, M3004, M3005, M3006, M3007, M3011, M3014, M3024, M3025, M3026, M3027, M3037, M3044-V, M3044-WV, M3045-V, M3045-WV, M3046-1.8mm, M3046-V, M3104-L, M3105-L, M3106-L, M3113-R, M3113-VE, M3114-R, M3114-VE, P8513, P8514, M3203, M3204, M5013, M5014, M7001, M7010, M7014, M7011, M7016, P1244, P1254, P1264, P1311, P1343, P1344, P1346, P1347, P1353, P1354, P1355, P1357, P1364, P1365, P1365Mk_II, P1405, P1405-LE_Mk_II, P1425, P1425-LE_Mk_II, P1427, P1428-E, P1435, P3214, P3215, P3224, P3225, P3224_LV_LVE_Mk_II, P3225_LV_LVE_Mk_II, P3224_V_VE_Mk_II, P3225_V_VE_Mk_II, P3227, P3228, P3301, P3304, P3343, P3344, P3346, P3353, P3354, P3363, P3364, P3365, P3367, P3384, P3707-PE, P3904, P3904-R, P3905, P3915-R, P5414-E, P5415-E, P5512, P5512-E, P5514, P5514-E, P5515, P5515-E, P5522, P5522-E, P5532, P5532-E, P5534, P5534-E, P5544, P5624-E, P5624-E-Mk_II, P5635-E, P5635-E-Mk_II, P7210, P7214, P7216, P7224, P7701, P8221, Q1602, Q1604, Q1614, Q1615, Q1635, Q1635-E, Q1615Mk_II, Q1659, Q1755, Q1755-PT, Q8722-E, Q1765-EX, Q1765-LE, Q1765-LE-PT, Q1775, Q1910, Q1921, Q1922, Q1931-E, Q1931-E-PT, Q1932-E, Q1932-E-PT, Q1941-E, Q1941-E-PT, Q1942-E, Q1942-E-PT, Q1942-EX, Q2901-E, Q2901-E-PT, Q2901-EX, Q3504, Q3505-Mk_II, Q3505, Q3615, Q3617, Q3708-PVE, Q3709-PVE, Q6000-E, Q6000-E-Mk_II, Q6032, Q6032-C, Q6032-E, Q6034, Q6034-C, Q6034-E, Q6035, Q6035-C, Q6035-E, Q6042, Q6042-C, Q6042-E, Q6042-S, Q6044, Q6044-C, Q6044-E, Q6044-S, Q6045, Q6045-C, Q6045-C-Mk_II, Q6045-E, Q6045-E-Mk_II, Q6045-Mk_II, Q6045-S, Q6045-S-Mk_II, Q6052, Q6052-E, Q6054, Q6054-E, Q6055, Q6055-C, Q6055-E, Q6055-S, Q6114-E, Q6115-E, Q6128-E, Q6155-E, Q7401, Q7404, Q7406, Q7411, Q7414, Q7424-R, Q7424-R-Mk_II, Q7436, Q8414-LVS, Q8631-E, Q8632-E, Q8665-E, Q8665-LE, V5914, V5915

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