

CVE-2016-6255 & CVE-2016-8863 (libupnp)

Source:

- [CVE-2016-6255](#)
Portable UPnP SDK (aka libupnp) before 1.6.21 allows remote attackers to write to arbitrary files in the webroot via a POST request without a registered handler.
- [CVE-2016-8863](#)
Heap-based buffer overflow in the create_url_list function in gena/gena_device.c in Portable UPnP SDK (aka libupnp) before 1.6.21 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a valid URI followed by an invalid one in the CALLBACK header of an SUBSCRIBE request.

Overview

UPnP (Universal Plug and Play) is a discovery protocol used by clients to easily find devices (services) on the network. Axis products include the imported open source package libupnp. A malicious client on the network could potentially exploit known vulnerabilities in libupnp (versions prior to version 1.6.21). It is potentially possible for a skilled adversary to develop an exploit that executes arbitrary code on these devices.

Risk assessment

An adversary with network access to Axis devices may be able to attack the UPnP agent. This may result in the UPnP agent being restarted with limited negative impact (temporary Denial of Service). A skilled and motivated adversary may be able to successfully achieve remote code execution. A successful remote code execution attack will not execute as a privileged user, limiting possible scope of negative impact. There are no known exploits (e.g. scripts or binaries) that target Axis devices specifically. Axis devices behind a NAT router or local network are at low risk as UPnP traffic does not normally propagate outside the NAT'ed environment.

Risk mitigation

As a precaution, customers are advised to update to the latest version (see below). The risks are also mitigated if UPnP is disabled in the devices. [Axis Hardening Guide](#) recommends disabling UPnP as soon as they are discovered and deployed in a system.

Patched Firmware and Models

Patched firmware for affected products is available for download at <https://www.axis.com/support/firmware>. The release notes for newly patched firmware will mention "Updated UPnP". Note that some release notes may not include reference to "UPnP", which would mean the vulnerability was already corrected in this version (example 7.30 and higher).

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.

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