RBS-2018-003

Axis Products Management Web Interface Multiple Vulnerabilities

Table of Contents

Vendor / Product Information

Axis Communications is a large Swedish-based company providing various network video solutions and with offices around the world. Their products are widely used and installed in public places and areas such as retail chains, airports, trains, motorways, universities, prisons, casinos, and banks.

Vulnerable Program Details

Details for tested products and versions:

Vendor:	Axis Communications AB
Product:	AXIS A1001 Network Door Controller
Version:	1.45.0 and 1.60.0

NOTE: Other product models and versions than the one listed above are affected. A more complete list of impacted product models can be found in Appendix A.

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Impact

Axis devices provide a web-based management interface for configuring them or access various resources and network video feeds. Multiple CGI scripts accessible via this web interface have vulnerabilities that allow authenticated, remote users to delete arbitrary files, cause buffer overflows, or execute shell commands with higher privileges. As the devices are vulnerable to cross-site request forgery attacks, these vulnerabilities may also be exploited by tricking logged-in users into visiting a malicious website. The devices were also found to bundle older versions of libupnp with publicly known vulnerabilities.

Vulnerability Details

Multiple CGI Scripts Remote Command Execution

Multiple CGI scripts accessible within the web-based management interface are vulnerable to shell command injection. The following scripts and parameters are vulnerable:

Affected CGI Script	Affected Parameter(s)
axis-cgi/httptest.cgi*	address, username, password, proxyaddress, proxyport, and proxylogin
axis-cgi/smtptest.cgi*	user, pass, popuser, poppass, subject, and body
axis-cgi/streamcache/streamcache.cgi	id
axis-cgi/ftptest.cgi	username and password

* Only version 1.45.0 of the tested A1001 device is impacted and not the later version 1.60.0

local_del.cgi CGI Script Path Traversal Remote File Deletion

Axis devices provide the local_del.cgi CGI script that is designed to delete files within the web root. The CGI script is e.g. called via fileUpload.shtml when attempting to upload files. The problem is that the CGI script does not sanitize file paths and is vulnerable to path traversal attacks. With a specially crafted request, an authenticated, remote attacker can delete arbitrary files on the device.

configuration.cgi Content-Length Header Remote Heap Buffer Overflow

Axis devices provide the axis-cgi/datacollection/configuration.cgi CGI script to configure various data collection settings. The CGI script does not properly validate the ‘Content-Length’ header for HTTP PUT requests before allocating a heap buffer based on its value. This may allow an authenticated, remote attacker to cause a heap-based buffer overflow.

file_upload Binary Filename Handling Remote Stack Buffer Overflow

Axis devices have a binary named file_upload (also known as file_cache), which is used to handle file uploads to the device e.g. via the axis-cgi/upload_file.cgi CGI script. The binary does not perform proper bounds checks when handling overly long filenames, which may allow an authenticated, remote attacker to cause a stack-based buffer overflow.

Web Interface Multiple Actions CSRF

HTTP requests to various functionality provided by the web-based management interface do not require multiple steps, explicit confirmation, or a unique token when performing sensitive actions. By tricking a user into following a specially crafted link, an attacker can perform cross-site request forgery (CSRF) attack. This can be exploited to cause the victim to perform a wide variety of sensitive actions on the device or be combined with the vulnerabilities described above to execute shell commands on the device.

Other Discoveries

During the review of the A1001 Network Door Controller we noticed various other issues that were also reported to Axis. These are either minor concerns that we do not really consider vulnerabilities or related to use of vulnerable libraries, where we did not discover the original vulnerability.

Vulnerable Version of the Portable UPnP SDK (libupnp)

Both of the tested versions of the A1001 Network Door Controller along with a long list of other Axis devices bundle a vulnerable version, 1.6.19, of the Portable UPnP SDK (libupnp). This is affected by CVE-2016-8863[1] and CVE-2016-6255[2].

After we informed Axis about their devices bundling this vulnerable 3rd party component, they released a separate security advisory[3] and fixes for these two vulnerabilities in November 2017.

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8863
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6255
[3] https://www.axis.com/files/faq/Advisory_libupnp_CVE-2016-6255_CVE-2016-8863.pdf

Unauthenticated Access To axis-cgi/prod_brand_info/getbrand.cgi

The axis-cgi/prod_brand_info/getbrand.cgi CGI script is accessible to unauthenticated users. This discloses Axis model information. Such system information disclosures are sometimes reported as a minor security issue, so it is being included here for the sake of completeness.

Axis Communications currently have no plans to address this.

pwdroot.cgi Remote Command Execution Weakness

Axis devices provide the axis-cgi/pwdroot/set_language.cgi CGI script for configuring the language on the device. The CGI script redirects to pwdroot.cgi when called, which then invokes /usr/html/axis-cgi/language.cgi with the supplied query string as argument via a system() call. As no validation is performed on the query string, this allows injecting and executing arbitrary shell commands on the device.

During our testing, we concluded that this is only possible during the initial device setup before a root password has been set i.e. when the device is in its factory default state. Any remote attacker with access to the device in this state would already constitute a significant security problem.

Axis Communications considers the risk limited and currently have no plans to address this.

Solution

Some of these vulnerabilities are already fixed in the latest versions of the impacted products. The vendor plans to address most of the remaining vulnerabilities during Q2 2018[4].

The vendor does not plan to address the CSRF vulnerability, but has published a separate security advisory[5] with various recommendations.

References

RBS:	RBS-2018-003[6]
VulnDB:	181030, 181031, 181032, 181033, 181034, 181035, 181036, 181038

Timeline

2017-08-16	Vulnerabilities discovered.
2017-10-09	Vulnerabilities reported to the vendor.
2017-10-10	Response from the vendor.
2017-11-29	The vendor issues an advisory and fixes for the libupnp vulnerabilities. Alerts are sent to RBS VulnDB clients.
2018-05-22	The vendor issues an advisory. Alerts are sent to RBS VulnDB clients.
2018-05-23	Publication of this vulnerability report.

[4] https://www.axis.com/files/faq/Advisory_ACV-122371-Mult-Vuln.pdf
[5] https://www.axis.com/files/faq/Advisory_Cross-Site_Request_Forgery.pdf
[6] https://www.riskbasedsecurity.com/research/RBS-2018-003.pdf

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established to support organizations with the technology to turn security data into actionable information and a competitive advantage. We do so by enhancing the research available and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database in the world. Available as feature-rich SaaS portal or powerful API. Vendor evaluations including our Vulnerability Timeline and Exposure Metrics (VTEM), Cost of Ownership ratings, Code Maturity, and Social Risk Scores.

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss. It also allows monitoring of domains for data breaches and leaked credentials as well as implementing a continuous vendor management program with our PreBreach data.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.

Appendix A: Impacted Axis Product 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, 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, 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, Q1615/Mk 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