RBS-2016-001

Multiple DVRs Web Interface Hardcoded Credentials Remote Authentication Bypass

Table of Contents

Vendor / Product Information

Zhuhai RaySharp Technology is a Chinese manufacturer of CCTV systems including stand-alone DVRs allowing real-time recording and viewing of feeds on multiple channels. The vendor's mission is to "*provide easy-to-install, simple-to-operate, high-quality and competitive-priced line of video surveillance products and let people feel safe in their daily life and work*"[1].

While based in China, the company's products are available worldwide. Supposedly, "*more than 60,000 units DVR are exported every month & delivered to all over the world*"[1]. Furthermore, the firmware used in the company's own DVR product line is also sold to a large number of DVR OEM vendors located in e.g. Europe and USA.

Vulnerable Program Details

DVRs offered by the following vendors have been confirmed vulnerable:

Vendor	Vendor Website
Zhuhai RaySharp Technology Co., Ltd.	http://www.raysharp.cn/en/
LOREX (Division of FLIR Commercial Systems)	https://www.lorextechnology.com/
König	http://www.konigelectronic.com/
DEFENDER	http://www.defender-usa.com/
DSP COP / COP-USA	http://www.cop-usa.com/
KGuard Security	http://www.kguardsecurity.com/
Swann	http://www.swann.com/

Fig. 1: Vendors confirmed to sell affected DVRs

NOTE: Many other OEM vendors are using firmware from Zhuhai RaySharp, as also covered by previous reports of vulnerabilities in the Raysharp DVR firmware[2]. See Appendix A for a list of vendors that may offer affected DVRs.

Credits

Carsten Eiram, Risk Based Security
Twitter: @CarstenEiram
Twitter: @RiskBased

[1] http://www.raysharp.cn/en/about-50.html
[2] https://community.rapid7.com/community/metasploit/blog/2013/01/28/ray-sharp-cctv-dvr-password-retrieval-remote-root

Impact

DVRs based on the Zhuhai RaySharp DVR firmware provide a web-based management interface for users to manage the device, view feeds from connected surveillance cameras, and use the PTZ (Pan-Tilt-Zoom) controls. It was found that the interface contains hardcoded credentials that allow anyone to easily access the device.

Fig 2: Map from Shodan.io showing the prevalence of affected DVRs around the world

Based on searches using Shodan.io[3], there are about 36.000 to 46.000 affected Internet-connected devices. About half of these are located in USA with the remaining Top 5 countries being UK, Canada, Mexico, and Argentina in that order.

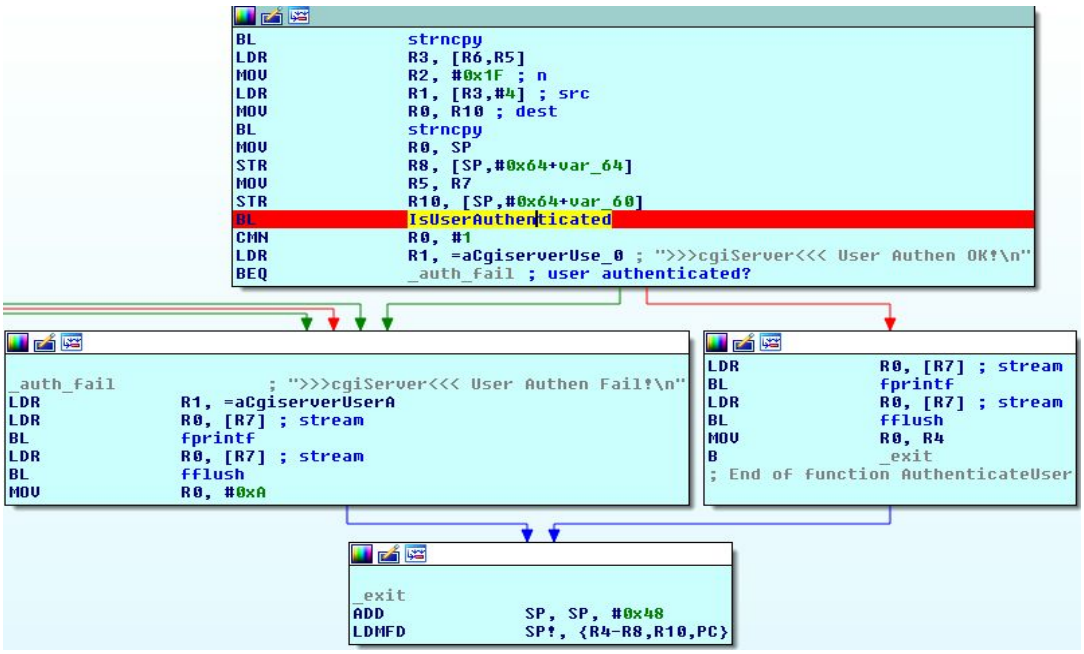
Vulnerability Details

In 2013 various vulnerabilities that allowed bypassing authentication by connecting directly to TCP port 9000 were reported[4] in these DVRs. In 2015 some of the issues were rediscovered[5] by another researcher. In both cases, the approach was to bypass authentication by communicating directly with the service listening on TCP port 9000 instead of the web interface.

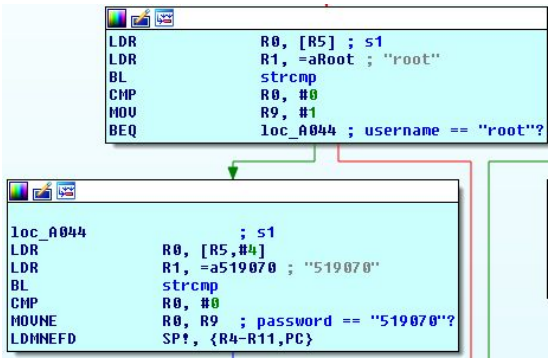
When encountering one of these DVRs, we decided to analyze the web interface authentication process to determine, if there was a simpler way to gain unauthorized access. While analyzing the `/www/cgi/cgiServer` binary, we noticed that the authentication process specifically checked for the username "root" and password "519070". The same code was found in the `/www/cgi/RscgiServer` binary.

[3] https://www.shodan.io/
[4] http://console-cowboys.blogspot.com/2013/01/swann-song-dvr-insecurity.html
[5] http://seclists.org/bugtraq/2015/Mar/34

The `main()` function of the CGI script calls a function to authenticate the user. Within this function, another function is eventually called to handle the authentication and return the result.



The function retrieves the user-supplied credentials and calls a function to check them. Within this function, part of the code specifically checks if the supplied username is “root” and the password is “519070”.



If these credentials are supplied, full access is granted to the web interface.

NOTE: During completion of this report, a few older reports[6,7] mentioning the password were found. The reports suggest any username may be used to log in combined with the password. Testing did not confirm this, though it may have been true for older devices. All tested products required a username of “root” to be supplied.

[6] http://www.amazon.com/review/R19KW1BWZX7OJZ/
[7] http://www.cctvforum.com/viewtopic.php?f=56&t=23410

Solution

We are not currently aware of any fixes from Zhuhai RaySharp. However, DEFENDER has reportedly issued a fix and a few other vendors may also have released fixes or are planning to. Please refer to the US-CERT vulnerability note for a list of affected vendors, fix status, and responses.

References

RBS:	RBS-2016-001[8]
VulnDB:	134624
CVE:	CVE-2015-8286[9]
US-CERT VU:	899080[10]

Timeline

2015-09-06	Vulnerability discovered.
2015-09-09	Vulnerability reported to US-CERT
2015-10-29	US-CERT provides status update that all known affected vendors have now been contacted.
2015-11-18	US-CERT provides status update that DEFENDER has responded that updated firmware was released end of September 2015 and is available to any customer that contacts Customer Service and asks.
2015-12-21	US-CERT provides status update that Zhuhai RaySharp has finally been responsive and are reviewing the report.
2016-01-18	Status update requested.
2016-01-29	US-CERT provides status update that no additional information has been received from Zhuhai RaySharp and that the vendors in general haven't been responsive except a couple of them e.g. Swann that hinted they were working on their own patches.
2016-01-30	Due to general lack of responsiveness from the affected vendors, a disclosure date of 2016-02-17 is agreed upon with US-CERT.
2016-02-17	Publication of this vulnerability report.

[8] https://www.riskbasedsecurity.com/research/RBS-2016-001.pdf
[9] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8286
[10] https://www.kb.cert.org/vuls/id/899080

Appendix A: Possibly Affected Vendors

Analysis of `mediaport.cgi` from a DEFENDER device using another firmware version also based on code from Zhuhai RaySharp, but not immediately vulnerable to the hardcoded credentials revealed a long list of vendors using the OEM firmware. Except from the vendors listed in the “Vulnerable Program Details” section, no other vendors have been confirmed affected. However, it cannot be ruled out that some of the vendors listed here may have sold or are selling DVRs using the vulnerable firmware versions.

```
.data:000115EC off_115EC      DCD aLorex            ; DATA XREF: sub_8ED0+4C o
.data:000115EC                                      ; .text:off_8F50 o ...
.data:000115EC                                      ; "LOREX"
.data:000115F0                DCD aPanda            ; "PANDA"
.data:000115F4                DCD aUrmet            ; "URMET"
.data:000115F8                DCD aOwl              ; "OWL"
.data:000115FC                DCD aRaysharp         ; "RAYSHARP"
.data:00011600                DCD aDeapa            ; "DEAPA"
.data:00011604                DCD aCop              ; "COP"
.data:00011608                DCD aSwann            ; "SWANN"
.data:0001160C                DCD aBcs              ; "BCS"
.data:00011610                DCD aZmodo            ; "ZMODO"
.data:00011614                DCD aKguard           ; "KGUARD"
.data:00011618                DCD aSoyo             ; "SOYO"
.data:0001161C                DCD aBolide           ; "BOLIDE"
.data:00011620                DCD aQsee             ; "QSEE"
.data:00011624                DCD aJ2000            ; "J2000"
.data:00011628                DCD aCosmos           ; "COSMOS"
.data:0001162C                DCD aEyeforce         ; "EYEFORCE"
.data:00011630                DCD aGsb              ; "GSB"
.data:00011634                DCD aGreatek          ; "GREATEK"
.data:00011638                DCD aLuxvision        ; "LUXVISION"
.data:0001163C                DCD aProtectron       ; "PROTECTRON"
.data:00011640                DCD aVeotex           ; "VEOTEX"
.data:00011644                DCD aSecurity         ; "SECURITY"
.data:00011648                DCD aNormal           ; "NORMAL"
.data:0001164C                DCD a30days           ; "30DAYS"
.data:00011650                DCD aDefender         ; "DEFENDER"
.data:00011654                DCD aSvat             ; "SVAT"
.data:00011658                DCD aAlphatech        ; "ALPHATECH"
.data:0001165C                DCD aSecura           ; "SECURA"
.data:00011660                DCD aHiviewer         ; "HIVIEWER"
.data:00011664                DCD aSateko           ; "SATEKO"
.data:00011668                DCD aEaglestar        ; "EAGLESTAR"
.data:0001166C                DCD aHoneywell        ; "HONEYWELL"
.data:00011670                DCD aNovicom          ; "NOVICOM"
.data:00011674                DCD aLegrand          ; "LEGRAND"
.data:00011678                DCD aWinplus          ; "WINPLUS"
.data:0001167C                DCD aZenon            ; "ZENON"
.data:00011680                DCD aFlir             ; "FLIR"
.data:00011684                DCD aElkron           ; "ELKRON"
.data:00011688                DCD aAnguatech        ; "ANGUATECH"
.data:0001168C                DCD aOdeon            ; "ODEON"
```

```
.data:00011690              DCD aIntelligence      ; "INTELLIGENCE"
.data:00011694              DCD aIqcctv           ; "IQCCTV"
.data:00011698              DCD aBalandi           ; "BALANDI"
.data:0001169C              DCD aBright           ; "BRIGHT"
.data:000116A0              DCD aIxtrima          ; "IXTRIMA"
.data:000116A4              DCD aKonig            ; "KONIG"
.data:000116A8              DCD aCocoon            ; "COCOON"
.data:000116AC              DCD aSky              ; "SKY"
.data:000116B0              DCD aRci             ; "RCI"
.data:000116B4              DCD aMaxx             ; "MAXX"
.data:000116B8              DCD aSentient          ; "SENTIENT"
.data:000116BC              DCD aStarlife         ; "STARLIFE"
.data:000116C0              DCD aCeltech           ; "CELTECH"
.data:000116C4              DCD aIpekam            ; "IPEKAM"
```

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 in early 2011 to better support the many users and initiatives of the Open Security Foundation - including the OSVDB and DataLossDB projects. RBS was created to transform this wealth of security data into actionable information 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. Available as feature-rich SaaS portal or powerful API

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.

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.