RBS-2014-003

Asante VMS ActiveXCoat ActiveX Control ConnectToVMS() Method Heap Buffer Overflow

Table of Contents

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.

Vulnerable Program Details

Details for the tested product and version:

Vendor:	UIC Corporation
Product:	Asante VMS
Version:	2.3
Component:	ActiveXCoat.ocx
File version:	1.4.0.0

References

RBS:	RBS-2014-003
OSVDB / VulnDB:	108488[1]
CVE:	N/A

Credits

Carsten Eiram, Risk Based Security

Twitter: @CarstenEiram
Twitter: @RiskBased

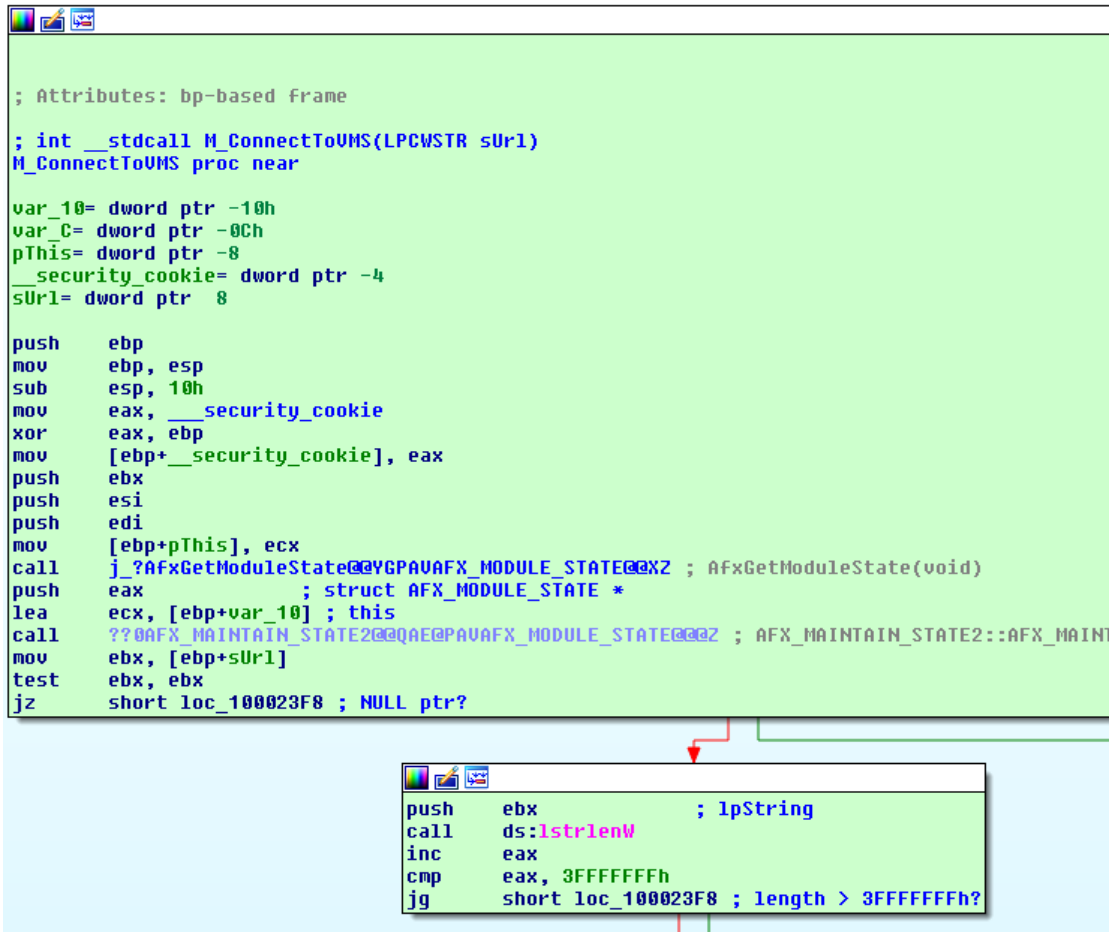
[1] http://www.osvdb.org/show/osvdb/108488

Vulnerability Details

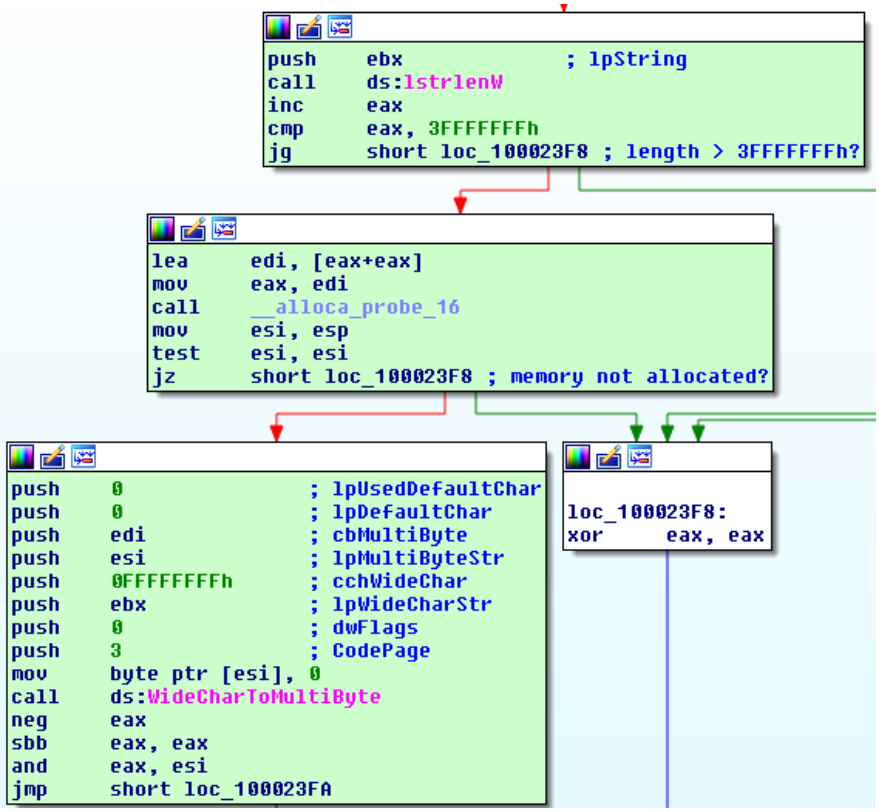
Asante VMS is a video management software solution for displaying feeds from multiple surveillance cameras. Viewing the feeds is possible via Internet Explorer by accepting to install a bundled ActiveX control, Uniform Media ActiveX Coat Control (ActiveXCoat.ocx), on a client system when accessing the default web page for the first time.

One of the supported methods by the ActiveX control is ConnectToVMS(), which takes a single string (sURL) as argument.

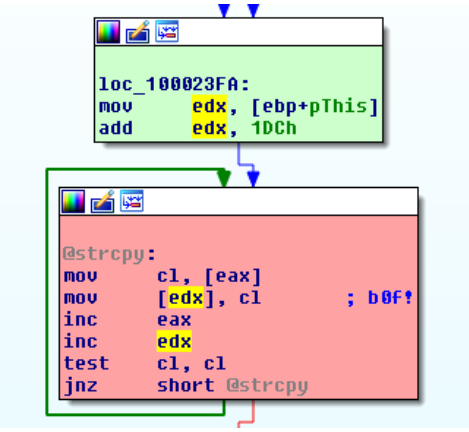
When supplying the 'sURL' string argument, the function in ActiveXCoat.ocx that handles calls to the ConnectToVMS() method checks that the length is no longer than 3FFFFFFFh.



If smaller, stack space is allocated accordingly using _alloca_probe_16, and the string is converted through a call to WideCharToMultiByte().



The resulting string is then copied straight into a 260 byte destination buffer at offset 1DCh of an object on the heap using an inlined strcpy() without performing any bounds checks. This allows triggering a heap-based buffer overflow and gaining control of the program flow.



Solution

No fix is available from the vendor, and the product is now end-of-life. Users should delete the ActiveX control, and set the kill-bit for CLSID {CC4A36F1-0CDA-48B5-BEFF-65A77B02CBCB}.

Timeline

2014/05/18	Vulnerability discovered.
2014/05/28	Vulnerability reported to vendor.
2014/05/28	Vendor responds that info has been passed on to the engineering management team, and that the product is reaching end-of-life.
2014/06/30	OSVDB entry published and details made available on VulnDB[2].
2015/04/29	Publication of this vulnerability report.

[2] https://www.riskbasedsecurity.com/risk-data-analytics/vulnerability-database/