RBS-2014-001

Schneider Electric CitectSCADA Citect.Platform.Transport.dll IdentifyMessageAdapter::ExtractIdentifyMessage Function Invalid IdentifyMessage Handling DoS

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:	Schneider Electric
Product:	CitectSCADA
Version:	7.20 and 7.20 SP1
Component:	Citect.Platform.Transport.dll
File version:	2.1.0.556
Platform:	Windows Server 2003 R2 Enterprise Edition

NOTE: In addition to the tested version, the vendor reports that the vulnerable library is bundled with the following products: SCADA Expert Vijeo Citect, Vijeo Citect, PowerSCADA Expert, and PowerLogic SCADA. For full details about affected versions, please see the ICS-CERT advisory.

References

RBS:	RBS-2014-001
OSVDB / VulnDB:	103434[1]
CVE:	CVE-2013-2824 CVE-2013-2605
ICS-CERT:	ICSA-13-350-01A[2]

Credits

Carsten Eiram, Risk Based Security

Twitter: @CarstenEiram
Twitter: @RiskBased

[1] http://www.osvdb.org/show/osvdb/103434
[2] https://ics-cert.us-cert.gov/advisories/ICSA-13-350-01A

Vulnerability Details

Schneider Electric CitectSCADA provides the Citect Time Synchronization Service, TimeSyncService.exe, which listens on TCP port 2088 (not enabled by default). The service is used to synchronize the system's clock against a specified time source or act as a time source.

When the service receives messages, processing primarily occurs in Citect.Platform.Transport.dll. Received packets are expected to contain so-called IdentifyMessage content used to identify various information about a client. This is extracted from the packet by calling the IdentifyMessageAdapter::ExtractIdentifyMessage() function.

Within this function, a certain value in the packet is eventually checked to determine if matching one of two expected hash codes. In case the value does not match either of these, the content is considered invalid and an InvalidDataException is thrown.

However, neither IdentifyMessageAdapter::ExtractIdentifyMessage() nor any other called functions in Citect.Platform.Transport.dll or TimeSyncService.exe register an exception handler to deal with such exceptions. This can be exploited to cause the service to terminate by sending any packet not matching the expected IdentifyMessage format (e.g. just 200 ‘A’ characters).

Citect Time Synchronization Service is the only known attack vector, but as the affected component is a library, Citect.Platform.Transport.dll, the vulnerability may be triggered through other vectors.

Additional Issues

Upon being contacted, the vendor was encouraged to check the code for similar problems, which were uncovered in the PacketAdapterV100::ReadPacketHeader(), PacketAdapterV100::ReadMessage(), PacketAdapter::ReadMessage(), and PacketAdapter::ReadPacketHeader() functions. These were addressed in the latest version of the library across various products. It should be noted that vectors to trigger these potential issues are not currently known, but may exist.

Solution

Vendor:	Schneider Electric
Product:	CitectSCADA
Version:	7.20 SP2
Component:	Citect.Platform.Transport.dll
File version:	2.1.2.67

NOTE: The fix listed above only addresses the one vulnerability proven to have a valid attack vector. It is unclear when it was fixed in other affected products. Also, the additional potential issues were addressed by patches for SCADA Expert Vijeo Citect v7.40, Vijeo Citect v7.30 SP1, Vijeo Citect v7.20 SP4, CitectSCADA v7.40, CitectSCADA v7.30 SP1, CitectSCADA v7.20 SP4, PowerSCADA Expert v7.30 SR1, and PowerLogic SCADA v7.20 SR1.

Timeline

2013/10/09	Vulnerability discovered in version CitectSCADA 7.20.
2013/10/10	Vulnerability reported to ICS-CERT
2013/10/21	Patch provided for testing.
2013/10/23	Further testing by RBS uncovers that the provided patch has no effect, as the vulnerability apparently was silently fixed by version 7.20 SP2.
2013/12/16	ICS-CERT publishes advisory to US-CERT Secure Portal library.
2014/02/18	OSVDB entry published and details made available on VulnDB[3].
2014/01/24	Fixes released.
2014/02/26	ICS-CERT publishes advisory.
2015/04/29	Publication of this vulnerability report.

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