RBS-2013-001

Rockwell Automation RSLinx Enterprise LogReceiver Service Datagram Handling Thread Exit Remote Denial of Service

Table of Contents

About Risk Based Security

Mission

To equip clients with the technology and customized risk-based consulting solutions to turn security data into information and information into a competitive advantage.

Background

Risk Based Security, Inc., incorporated in 2011, was established to better support the users/contributors to the Open Security Foundation, OSF, with the technology to turn security data into a competitive advantage.

The OSF's wealth of historical data, combined with the interactive dashboards and analytics offered by Risk Based Security provide a first of its kind risk identification and security management tool.

Risk Based Security further complements the data analytics with risk-focused consulting services to address industry specific information security and compliance challenges.

Discriminators

Risk Based Security offers a full set of analytics and user-friendly dashboards designed specifically to identify security risks by industry.

Risk Based Security is the only company that offers its clients a fully integrated solution – real time information, analytical tools and purpose-based consulting.

Unlike other security information providers, Risk Based Security offers companies comprehensive insight into data security threats and vulnerabilities most relevant to their industry.

Vulnerable Program Details

Vendor:	Rockwell Automation
Product:	RSLinx Enterprise
Version:	5.50.04 CPR 9 SR 5
Component:	LogReceiver.exe
File version:	5.50.4.19
Platform:	Windows Server 2003 R2 Enterprise Edition

References

RBS:	RBS-2013-001
OSVDB:	92048
CVE:	CVE-2012-4695
ICS-CERT:	ICSA-13-095-02
Rockwell:	537599

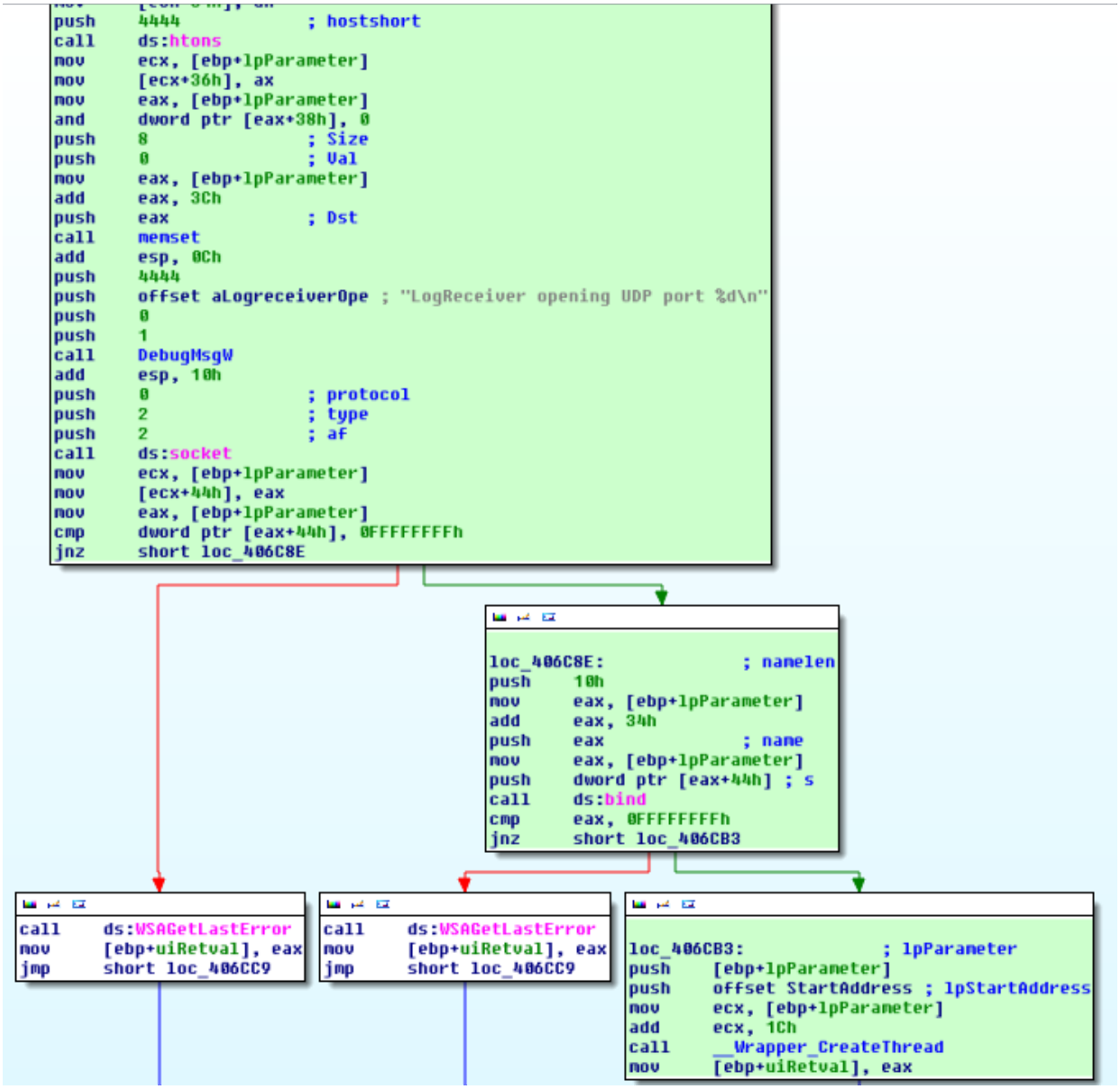
Credits

Carsten Eiram, Risk Based Security

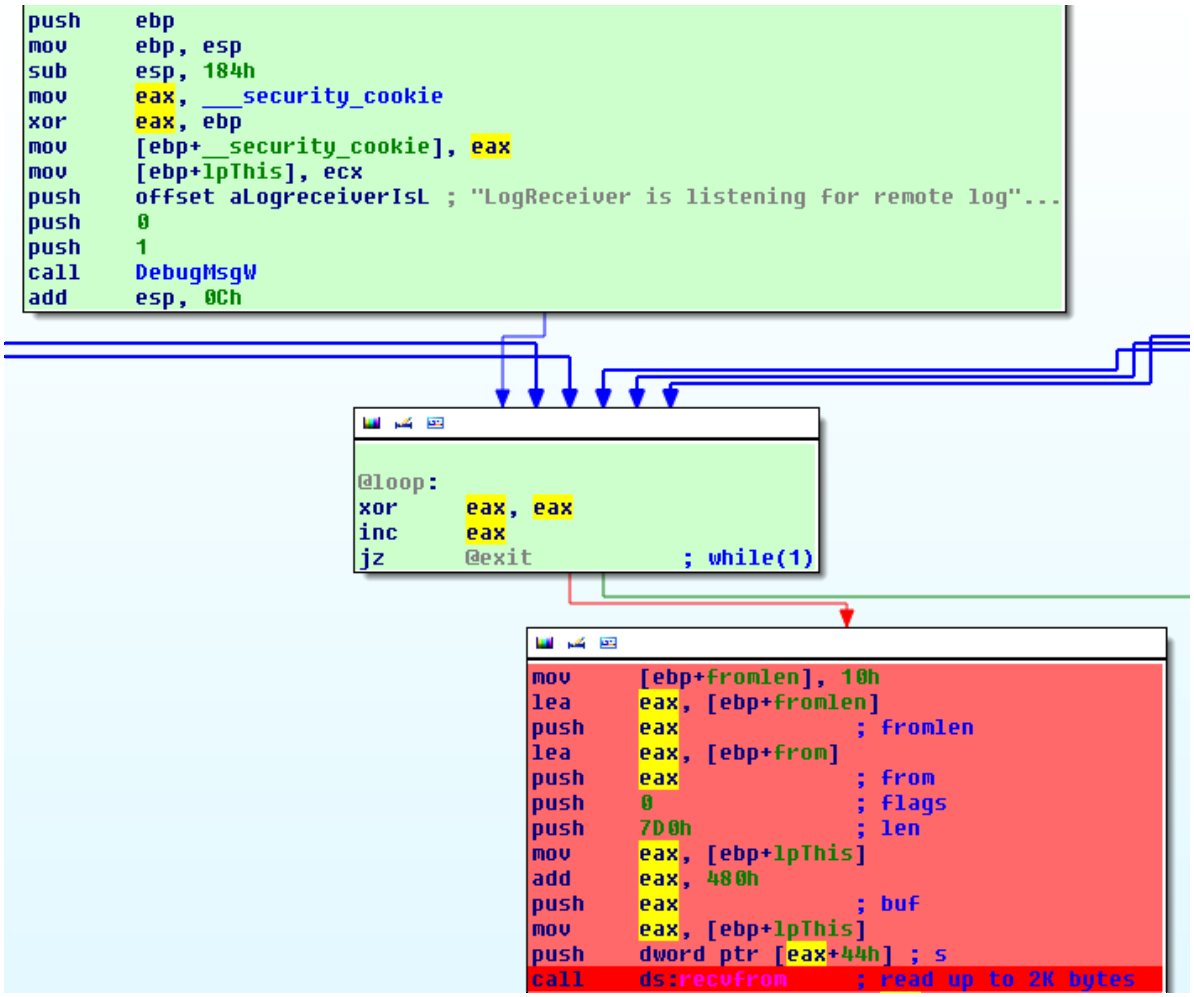
Twitter: @carsteneiram
Twitter: @riskbased

Vulnerability Details

RSLinx Enterprise provides the RSLinx Enterprise Network Event Log Service, LogReceiver.exe, which once it's started (disabled by default) binds to UDP port 4444 and creates a thread to log network events.

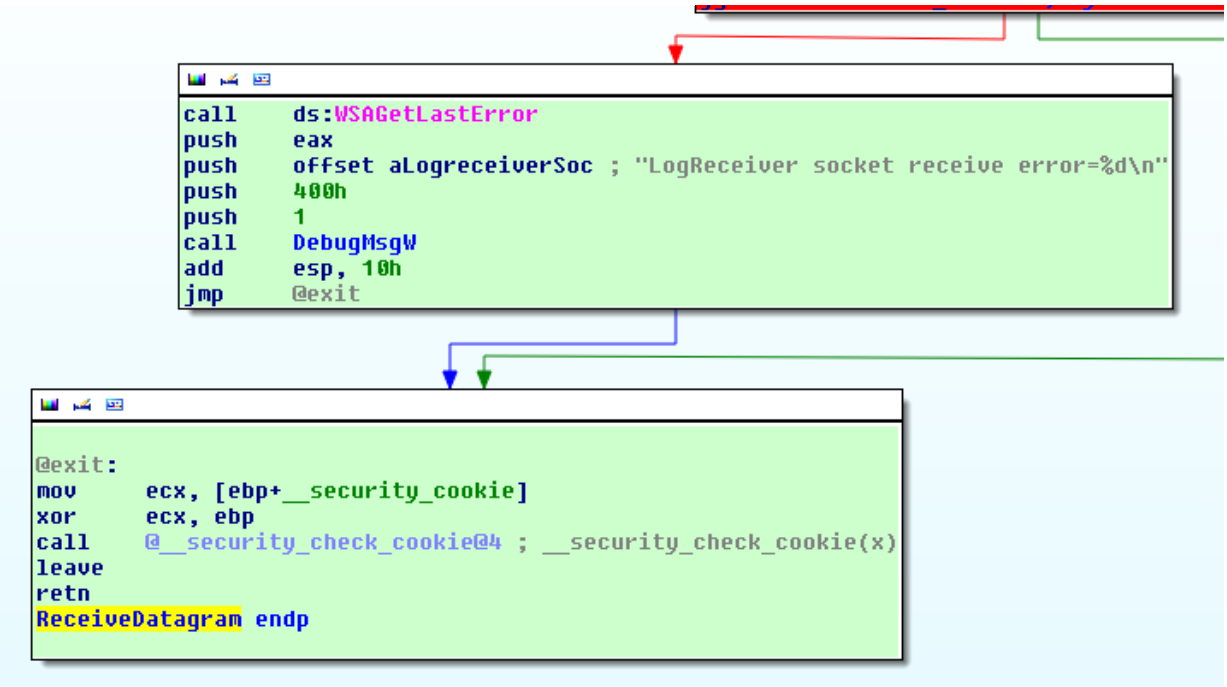


The logging of network events is done by entering an “infinite” loop in the new thread and then waiting for incoming datagrams.



Once data is received, the number of bytes is checked to ensure that one or more was received.

In case zero data is received, more than 2000 bytes is received, or some error occurs when calling recvfrom(), the function branches to log an error and then exits.



Since the function is running as a separate thread listening for incoming requests, but it's not restarted by the service if exiting, the service stops processing new incoming requests, though it is still bound to UDP port 4444. With a 0 or 2000+ byte datagram, a remote attacker can exploit this to cause the service to silently ignore incoming requests until restarted.

Solution

The vendor has released a patch, ID534705, which addresses the vulnerability by logging a socket receive error, but then jumping to the beginning of the loop to continue receiving data instead of exiting the thread.

Patched component:	LogReceiver.exe
Patched file version:	5.50.6.22

Timeline

2012/12/18	Vulnerability discovered.
2012/12/21	Vulnerability reported to ICS-CERT.
2013/01/08	Rockwell Automation acknowledges the vulnerability.
2013/02/08	Rockwell Automation provides status update.
2013/02/28	Rockwell Automation provides status update.
2013/03/15	Rockwell Automation provides status update.
2013/03/27	Rockwell Automation provides patches.
2013/04/05	Alerts published for OSVDB and RBS VulnDB Service[1]
2013/04/27	Publication of this vulnerability report.

[1] http://www.riskbasedsecurity.com/risk-data-analytics/vulnerability-database/