RBS-2013-002

Rockwell Automation FactoryTalk Services Platform RNADiagnostics Module Missing Size Field Validation 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:	FactoryTalk Services Platform
Version:	2.50 CPR9 SR5
Component:	RNADiagnostics.dll
File version:	2.50.0.10
Platform:	Windows Server 2003 R2 Enterprise Edition

References

RBS:	RBS-2013-002
OSVDB:	92057
CVE:	CVE-2012-4713, CVE-2012-4714[1]
ICS-CERT:	ICSA-13-095-02
Rockwell:	537599

Credits

Carsten Eiram, Risk Based Security

Twitter: @carsteneiram
Twitter: @riskbased

[1] ICS-CERT initially assigned two CVE identifiers, but based on additional dialogue one of these may be REJECTed with the other covering both issues.

Vulnerability Details

Rockwell Automation FactoryTalk Services Platform comes with FactoryTalk Diagnostics that allows storing and managing information about errors and changes occurring on FactoryTalk-enabled systems. One of the included components is `RNADiagnostics.dll`, which is e.g. used by the FactoryTalk Diagnostics CE Receiver service, `RNADiagReceiver.exe`, to parse received type 2 messages (specified by the initial word value in the datagram) from Windows CE devices on UDP port 4445 (disabled by default).

`RNADiagnostics.dll` contains flaws when parsing these messages that may allow a remote denial of service by crashing a service linked against the library. The issues are triggered when reading either of two size values within the stream and attempting to allocate memory based on these, as each specifies the number of following data structures in the stream.

In the case of the first value, it is multiplied by 16 and passed to operator new[] if no integer overflow occurred; else 0xFFFFFFFF is supplied.

```
mov     ecx, [ebp+lpoCDiag]
cmp     [ecx+CDiag.m_uiNumVariants], 0
jz      short loc_10018DE8
```

```
xor     ecx, ecx
mov     edx, [ebp+lpoCDiag]
mov     eax, [edx+CDiag.m_uiNumVariants]
mov     edx, 10h
mul     edx             ; int0f
seto    cl
neg     ecx
or      ecx, eax
push    ecx
call    mfc90u_265      ; mfc90u?operator new[]
add     esp, 4
mov     [ebp+lpMem], eax
mov     eax, [ebp+lpoCDiag]
mov     ecx, [ebp+lpMem]
mov     [eax+CDiag.m_lpArrVariants], ecx ; store ptr to allocated buffer
mov     [ebp+iIndex], 0
jmp     short @loop_init_variants
```

In the case of the second value, it is multiplied by 32 and adding 4, passing the result to operator new[] if no integer overflow occurred; else 0xFFFFFFFF.

```
mov     edx, [ebp+lpoCDiag]
mov     eax, [edx+CDiag.m_lpArrSomeStruct]
mov     ecx, [eax]
mov     [ebp+uiNumStructs], ecx
xor     ecx, ecx
mov     eax, [ebp+uiNumStructs]
mov     edx, 20h
mul     edx
seto    cl
neg     ecx
or      ecx, eax
xor     eax, eax
add     ecx, 4
setb    al
neg     eax
or      eax, ecx
push    eax
call    mfc90u_265      ; mfc90u!operator new[]
add     esp, 4
mov     [ebp+lpuiSomeCount], eax
mov     byte ptr [ebp+var_4], 5
cmp     [ebp+lpuiSomeCount], 0
jz      short loc_100194AE
```

In both cases, if the result is overly large or set to 0xFFFFFFFF due to an integer overflow occurring, operator new[] fails to allocate the specified amount of memory and throws an exception. However, as the exception is unhandled, the process linked against the library terminates.

An attacker can exploit this to terminate a service linked against the library e.g. the FactoryTalk Diagnostics CE Receiver by sending a specially crafted message where either of the two values is overly large, causing memory allocation to fail.

Solution

The vendor has released a patch, ID522048, which addresses the vulnerabilities by checking the values against the stream size read from the message before trying to allocate memory.

Patched component:	RNADiagnostics.dll
Patched file version:	2.50.0.33

Timeline

2012/12/10	Vulnerabilities discovered.
2012/12/12	Vulnerabilities reported to ICS-CERT.
2013/01/08	Rockwell Automation acknowledges vulnerabilities.
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[2]
2013/04/27	Publication of this vulnerability report.

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