Security Advisory AudioCodes Mediant family

AudioCodes Mediant family of multi-service business routers (MSBRs) offers service providers a range of all-in-one SOHO, SMB and SME routers combining access, data, voice and security into a single device. [1]
During our research we found a DoS, a XXS and CSRF vulnerability. Although we could gain access to quagga VTYs.

Affected Products:
- AudioCodes Mediant 500L-MSBR
- AudioCodes Mediant 500-MBSR
- AudioCodes Mediant M800B-MSBR
- AudioCodes Mediant 800C-MSBR

CVE-2019-9228 - SSH and TELNET DoS (connection slot exhaustion)
The management SSH and management TELNET features allow remote attackers to cause a denial of service (connection slot exhaustion) via 5 unauthenticated connection attempts, because the maximum number of unauthenticated clients that can be configured is 5.

Affected Versions:
F7.20A at least to 7.20A.252.062.
The vendor's position is that this is a design choice, because having a higher value would put a higher load on the system resources. There will be no fix, because the Risk is classified as acceptable.

Mitigation:
Restrict the access to the interfaces via Access Lists.

CVE-2019-9229 - Access to internal quagga interface with hard coded credentials
An internal interface exposed to the link-local address 169.254.254.253 allows attackers in the local network to access multiple quagga VTYs. Attackers can authenticate with the default password "1234" that cannot be changed, and can execute malicious and unauthorized actions.

Affected Versions:
F7.20A to F7.20A.251

Mitigation:
Update to F7.20A.252 or higher.

CVE-2019-9230 - Cross-site scripting
A cross-site scripting (XSS) vulnerability in the search function of the management web interface allows remote attackers to inject arbitrary JS or HTML code via the keyword parameter. This is possible because a wrong content-type header (text/html instead of application/json) is set.

Affected Versions:
F7.20A to F7.20A.253

Mitigation:
Update to F7.20A.254 or higher.

CVE-2019-9231 - Cross-Site Request Forgery
A Cross-Site Request Forgery (CSRF) vulnerability in the management web interface allows remote attackers to execute malicious and unauthorized actions, because CSRF Protection is not activated by default and the option is not documented in the user manual or security guidelines.

Affected Versions:
F7.2 to F7.2.202.307 and any Version shipped with version before F7.2.202.307.
The CSRF protection was implemented in version 7.2.202.307 but is not activated by default. The option is not documented in the Mediant 500L user manual or security guidelines. Devices shipped with version
7.2.202.307 and later have the option enabled by default. The option is not activated in an update.
Mitigation:

Update to F7.20A.202.307 or higher and activate the CSRF protection. The option could be enabled only by the upload of a ini file with the parameter "CSRFProtection=1"

Disclosure Timeline

2019/02/14 vendor contacted
2019/02/14 initial vendor response
2019/02/14 vendor informs about start of review process
2019/02/15 vendor requests further details
2019/02/15 further details provided
2019/02/18 vendor informs about detail analysis
2019/02/19 vendor confirmation, planned fixes and roadmap provided
2019/03/01 CVEs assigned
2019/06/28 vendor informs that planned fixes are published

External References:

[1]
https://www.audiocodes.com/solutions-products/products/multi-service-business-routers-msbrs

Credits:

Stefan Strobel
Stefan.Strobel@cirosec.de
cirosec GmbH
https://www.cirosec.de/en

Simon Winter
simon.winter95@web.de
Aalen University
https://www.hs-aalen.de/AudioCodes