HIMA Security Note
Ripple 20

Introduction/Background

18th of June 2020 the ICS-CERT has informed about security issues in a TCP/IP stack implementation. The security researchers of the company JSOF found 19 issues and called the sum of breaches "Ripple20".
The rather slim implementation of the stack is well suited for embedded devices. Therefore it is widely spread and may endanger devices e.g. in households, hospitals and industrial plants.

The position of HIMA

HIMA is a member of CERT@VDE. Due to this membership HIMA received information of the above mentioned security issues from the CERT@VDE at the 18th of June 2020. HIMA immediately investigated whether HIMA Products might be directly affected of Ripple20.
On 19th of June 2020 HIMA was able to inform CERT@VDE that **none** of the HIMA-products uses the vulnerable TCP/IP-Stack.
The detected issues have the highest possible CVSSv3 score which is 10.0. Due to this high severity HIMA decided to further investigate whether the described issues might also be effective in the TCP/IP-stacks of HIMA.
Fortunately **no** adverse security effects or safety complications are to be expected.

Further information

Further information is available from:
https://www.kb.cert.org/vuls/id/257161
https://www.us-cert.gov/ics/advisories/icsa-20-168-01

If you have specific questions regarding your HIMA systems, please contact support@hima.com for technical questions and security@hima.com for issues concerning automation security.