Nanometrics Centaur / TitanSMA Unauthenticated Remote Memory Leak Exploit

Title: Nanometrics Centaur / TitanSMA Unauthenticated Remote Memory Leak Exploit
Advisory ID: ZSL-2020-5562
Type: Local/Remote
Impact: System Access, DoS, Exposure of System Information, Exposure of Sensitive Information
Risk: (5/5)
Release Date: 15.02.2020

Summary

The Centaur digital recorder is a portable geophysical sensing acquisition system that consists of a high-resolution 24-bit ADC, a precision GNSS-based clock, and removable storage capabilities. Its ease of use simplifies high performance geophysical sensing deployments in both remote and networked environments. Optimized for seismicity monitoring, the Centaur is also well-suited for infrasound and similar geophysical sensor recording applications requiring sample rates up to 5000 sps.

The TitanSMA is a strong motion accelerograph designed for high precision observational and structural engineering applications, where scientists and engineers require exceptional dynamic range over a wide frequency band.

Description

An information disclosure vulnerability exists when Centaur and TitanSMA fail to properly protect critical system logs such as 'syslog'. Additionally, the implemented Jetty version (9.4.z-SNAPSHOT) suffers from a memory leak of shared buffers that was (supposedly) patched in Jetty version 9.2.9.v20150224. As seen in the aforementioned products, the 'patched' version is still vulnerable to the buffer leakage. Chaining these vulnerabilities allows an unauthenticated adversary to remotely send malicious HTTP packets, and cause the shared buffer to 'bleed' contents of shared memory and store these in system logs. Accessing these unprotected logfiles reveal parts of the leaked buffer (up to 17 bytes per sent packet) which can be combined to leak sensitive data which can be used to perform session hijacking and authentication bypass scenarios.

Vendor

Nanometrics Inc. - https://www.nanometrics.ca

Affected Version

Centaur <= 4.3.23
TitanSMA <= 4.2.20

Tested On

Jetty 9.4.z-SNAPSHOT

Vendor Status

[10.02.2020] Vulnerabilities discovered.
[10.02.2020] Vendor contacted.
[14.02.2020] No response from the vendor.
[15.02.2020] Public security advisory released.

PoC

centaur3.py

Credits

Vulnerability discovered by byteGoblin - <bytegoblin@zeroscience.mk>

References

[1] https://nvd.nist.gov/vuln/detail/CVE-2015-2080
[2] https://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5306.php
[3] https://packetstormsecurity.com/files/156387
[4] https://cxsecurity.com/issue/WLB-2020020091
[5] https://exchange.xforce.ibmcloud.com/vulnerabilities/176352
[6] https://www.exploit-db.com/exploits/48098
[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12134
[8] https://nvd.nist.gov/vuln/detail/CVE-2020-12134

Changelog

[15.02.2020] - Initial release
[19.02.2020] - Added reference [3], [4], [5] and [6]
[26.04.2020] - Added reference [7] and [8]

Contact

Zero Science Lab

Web: http://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Profiles**

-