APPROVED FOR RELEASE

Technical Report / Disclosure SUMMARY

Re-test of Viksfjord and Gator 3

mnemonic AS on behalf of the Norwegian Consumer Council

05.12.2017

Harrison Sand <harrison@mnemonic.no>
Tor E. Bjørstad <tor@mnemonic.no>

mnemonic
- securing your business

Executive summary

Context

mnemonic has performed a technical security assessment of the Gator 3 and Viksfjord smart watches, on request from and in cooperation with the Norwegian Consumer Council. The goal of the assessment has been to identify possible *security vulnerabilities* that may create a risk of personal information being leaked or disclosed, or otherwise cause harm to users of the device.

This is a follow-up assessment to evaluate whether changes made to the watches and their accompanying apps, responding to the disclosure of multiple vulnerabilities published in the **#WatchOut** report on October 18th 2017, adequately address the previously disclosed vulnerabilities.

The result of our re-test indicates that while *specific* issues have been mitigated, the *general* problems still persist. In some cases, changes have actually made the security of the products *worse*.

Other watches in the Viksfjord ecosystem, both other watch models using GPSFORALLE app, and watch models building on similar hardware models and using the SeTracker application (such as Wonlex), have not been re-tested in this iteration. However, based on our analysis in both reports, there are strong indications that these watches also are vulnerable, and that fixing the systematic security and privacy problems across the product range is likely to be difficult.

Gator 3: Summary of findings

mnemonic has discovered an Internet-exposed server containing IMEIs, user avatars, and voice messages for roughly 4000 Gator 3 users, publicly available and without any access control.

This finding puts a large amount of sensitive user data at serious risk, possibly both for Norwegian and international users. mnemonic immediately notified the Data Protection Authorities as well as Gator, and at time of publication, access to this server appears to have been restricted.

mnemonic was also able to modify the previously reported account takeover attack against the Gator 2 watch, to conduct a similar covert account takeover on the Gator 3. A successful attack enables pairing of an unauthorized app with the watch, and thus the ability to track and monitor an unsuspecting user as described in the #WatchOut report. Thus, the changes made in the Gator 3 watch and app do not adequately address the previously disclosed findings.

Finally, mnemonic has discovered a covert surveillance feature in the Gator 3 watch and app. The feature is hidden from the end users, but can be enabled by a knowledgeable technical user. Enabling the functionality allows an app user to covertly monitor the watch's microphone.

Viksfjord: Summary of findings

mnemonic was able to modify the previously reported account takeover attack against the Viksfjord, bypassing the mitigations that have been put in place. A successful attack enables pairing of an unauthorized app with the watch, and thus the ability to track and monitor an unsuspecting user as described in the #WatchOut report. The attack, as before, only requires knowledge of the device IMEI or phone number. Thus, the changes made to the Viksfjord watch and the introduction of the GPSFORALLE app do not adequately address the previously disclosed findings.

We have also observed unencrypted communications of personal data between the app and a backend server, as well as personal data being sent to a server located outside the EU, in Singapore.

Test objects

The assessment has been carried out using new test watches purchased by the Norwegian Consumer Council.

- Gator 3 watch purchased at XXL, using the Gator 3 Android app
- Viksfjord watch purchased at Enklere Liv in Nov 2017, using the GPSFORALLE Android app

Figure 1. Gator 3 watch from XXL

Figure 2. Viksfjord watch from Enklere Liv

Disclosure timeline

Re-testing was conducted in November 2017.

The Gator 3 findings were disclosed to the Norwegian Data Protection Authority, as well as Gator Norway (Gator AS), on November 16th.

The Viksfjord findings were disclosed to the Norwegian Data Protection Authority, as well as GPS for barn (Smartprodukt AS), on November 24th.

About the assessor

mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. Our expert team of security consultants, product specialists, threat researchers, incident responders and ethical hackers, combined with our Argus security platform ensures we stay ahead of advanced cyberattacks and protect our customers from evolving threats.

Acknowledged by Gartner as a notable vendor in delivering Managed Security Services, threat intelligence and advanced targeted attack detection, we are among the largest IT security service providers in Europe, the preferred security partner of the region's top companies and a trusted source of threat intelligence to Europol and other law enforcement agencies globally.

With intelligence-driven managed security services, more than 150 security experts, and partnerships with leading security vendors, mnemonic enables businesses to stay secure and compliant while reducing costs.