HMS Security Advisory Report

HMSSAR-2018-12-04-001

Publication date: 11 January 2019
Last update: 20 December, 2018

Overview

A cross-site scripting vulnerability has been identified in some Netbiter products which may be used by an attacker to bypass access control.

By exploiting the vulnerability, an attacker can inject client-side scripts into web pages.

Vulnerability reference: CVE-2018-19694

Impact

Successful exploitation of this vulnerability may allow a remote attacker to remotely log in to the target device and viewing data, change device configuration and send commands to connected devices.

Affected products and versions

- Netbiter WS100 – Firmware version 3.30.5 and previous
- Netbiter WS200 – Firmware version 3.30.4 and previous
- Netbiter EC150 – Firmware version 1.40.0 and previous
- Netbiter EC250 – Firmware version 1.40.0 and previous
- Netbiter LC310 – Firmware version 3.30.5 and previous
- Netbiter LC310 ThingWorx – Firmware version 2.00.07 and previous
- Netbiter LC350 – Firmware version 2.00.07 and previous
- Netbiter LC350 ThingWorx – Firmware version 2.00.07 and previous

Severity / CVSS Score

The CVSS [1]severity base score is 8.3, and the associated scoring vector is CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

HMS Recommendations

HMS recommends that the affected product is updated to the latest firmware version, corresponding to the firmware version in the list above, and then apply the security patch “Security_patch_2018_12_04” where the issue has been fixed. The security patch is not needed on Netbiter LC3XX firmware version > 2.00.07 where the issue has been fixed.

HMS also recommends putting the device behind a firewall and block port 80 and the optional port that is defined in Setup->Webserver->HTTP Settings->Extra webserver port – default 8080.

[1] CVSS is owned by FIRST and used by permission. https://www.first.org/cvss

Product updates

Firmwares and patches are available here: https://www.netbiter.com/support/file-doc-downloads.

Acknowledgements

HMS thanks Micha Borrmann from SySS GmbH for finding and notifying about the vulnerability in a controlled way.

Additional information

The vulnerability will be published by Micha Borrmann here: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19694

Applying the recommended security patch or firmware will also fix the vulnerability described in HMSSAR-2017-05-24-001.