HMSSAR-2017-05-24-001

Publication date: 24 May, 2017
Last update: 24 May, 2017

Overview

Bertin Jose and Fernandez Ezequiel has found a vulnerability in legacy NetBiter products. The vulnerability can make files in the product's internal filesystem accessible by non-authenticated users.

By using the vulnerability, the internal password file can be retrieved and then the password can be identified using a brute force attack of the password hash.

When the password is decoded the attacker is able to login to the device.

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® FGW200 – Firmware 3.21.2 and previous versions
- NetBiter® WS100 – Firmware 3.30.5 and previous versions
- NetBiter® EC150 – Firmware 1.40.0 and previous versions
- NetBiter® WS200 – Firmware 3.30.4 and previous versions
- NetBiter® EC250 – Firmware 1.40.0 and previous versions

Other NetBiter products like EC3XX and EC220 are not affected by this vulnerability.

The CVSS [1]severity base score is 10.0 (Critical), and the associated scoring vector is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/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_2017_05_24" where the issue has been fixed.

Before applying the patch, HMS recommended to reinstall the firmware and configuration in the case the device has been compromised and configuration files and/or user accounts has been changed.

Change all your passwords on the device.

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

Product updates

An update that patches the problem is available here: https://www.netbiter.com/support/file-doc-downloads

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

Additional information

The security issue was first reported here:
https://github.com/ezelf/industrial_Tools/tree/master/scadas_server_antiweb/LFI