SBC Security Advisory SEC-20180126

SECURITY ADVISORY

Vulnerability in Sangoma Session Border Controller (SBC) Products

Sangoma Advisory ID: SEC-20180126

Notice Date: January 26, 2018

CVE ID: CVE-2017-17430

Impact: (CVSS Score): 7.5

Product(s) Affected:

All Sangoma NetBorder and Vega Session Border Controllers, including NetBorder Carrier, NetBorder Enterprise, Vega Enterprise, and Vega SMB SBCs (Product SKUs beginning with SBCT- and SBCM-).

Software Versions Affected:

All software versions below 2.3.12

Fix:

This has been fixed in SBC Software version **2.3.12**.

Discovered By:

(Not Disclosed)

Overview:

A vulnerability exists that allows remote users to access the web GUI without entering proper credentials if the web GUI interface is exposed to the open internet. Allowing access to the web GUI via the internet is not recommended by Sangoma; however in our experience many customers choose to utilize this functionality. Once in the GUI, an attacker could change the settings or even disable the SBC, potentially without the immediate knowledge of its owner.

Update Instructions:

For more information on downloading and updating the SBC software, please see: https://wiki.freepbx.org/display/SBC/SBC+Downloads

Further Details:

The vulnerability allows an unauthorized user to access the remote Web GUI of the SBC if remote access is allowed. The unauthorized user may then make changes to the SBC configuration, or disable it, potentially without the owner's knowledge.

This has been fixed SBC software Version 2.3.12 (released December 14, 2017).

The Sangoma SBC team has now deemed this a **serious** security issue. The exploit had initially not been reported to have been exploited maliciously, but we immediately released an update to resolve it. Since that time, several customers have reported attacks and thus we have escalated the severity of the issue. We strongly encourage all users of Sangoma SBC products to upgrade to the latest software version as soon as possible.

If you believe your SBC has been compromised by this vulnerability, we strongly recommend that you contact Sangoma Support, who can review your SBC settings to be sure no malicious changes have been made or other vulnerabilities introduced.

Sangoma takes security seriously and requests that any security issues found in Sangoma products be reported to: security (at) sangoma (dot) com.

Workaround:

If you are running a vulnerable version of an Sangoma SBC product and are unable to immediately update the software, make sure that your web GUI is not accessible from the open Internet.