ComAp Vulnerability Disclosure

CA-VD-001

Webserver interfaces vulnerability

Security has always been a focus at ComAp, so our customers can rest assured ComAp always has and always will take the security of customers data and equipment seriously.

ComAp is committed to fix all reported security vulnerabilities quickly and carefully to protect the security and privacy of our users.

Affected products

- InternetBridge-NT
- Controllers with integrated communication module IB-COM:
  - InteliGen NTC BaseBox
  - InteliSys NTC BaseBox
  - InteliSys Gas
  - InteliSys GSC
  - products derived from the above
- IB-Lite

Vulnerability ID

ComAp ID: CA-VD-001

Summary

Recently there was a security issue found in the web server interfaces with certain older ComAp products. The requested web page was returned without a need to enter the Access Code.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.

CVSS v3 Base Score:	5.4 (Medium)
CVSS v3 Vector:	/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.1

Remediation

We have fixed the issue in InternetBridge-NT and IB-COM firmware. However, IB-Lite is an outdated product and we recommend replacing it with a newer controller solution (e.g. InteliLite 4 and plugin ethernet module). Your local contact representative can recommend which product is most suitable for your application.

Certain ComAp controllers include an integrated IB-COM module. We recommend updating these controllers to the latest firmware. These products include: InteliGen NTC BaseBox, InteliSys NTC BaseBox, InteliSys Gas and InteliSys GSC. The latest firmware for these controllers is available from the individual product pages on our website.

Links to the firmware update download, solving the security issue mentioned:

- InternetBridge-3.3.5 Link to FW, Link to NFL
- IB-COM-1.5.3 Link to FW, Link to NFL

Hardware versions of the above-mentioned products which include the fixed version of firmware already when shipped from factory:

- IS-NTC-BB: HW 2.0.1
- IG-NTC-BB: HW 2.0.1
- IG-NTC-BB 400Hz: HW 2.0.1
- IM-NTC-BB: HW 2.0.1
- InteliDrive BaseBox: ID1COMBBBAB: HW 2.2.1
- InteliGen GSC-C: IG2GSCCXBAB: HW 2.2.1
- InteliSys Gas: IS2GASXXBAB: HW 2.2.1
- InteliSys GSC-C: IS2GSCCXBAB: HW 2.2.1
- InternetBridge-NT 4G:
  - CM2IB4GABFB:HW 2.0.1;
  - CM2IB4GEBFB: HW 2.0.1;
  - CM2IB4GJBFB: HW 2.0.1
- InternetBridge-NT: IB-NT: HW 2.0.1

Vulnerability details

The issue was rooted in using an HTTP POST request instead of an HTTP GET request. When accessing a web page in a controller using a POST request without data, (instead of a GET request) the authentication with access code was bypassed, and the requested page was returned without a need to enter the Access Code. However, password protection for writing setpoints was not affected.

Mitigating Factors

Pay attention to the following recommendations and measures to increase the level of security of ComAp products and services.

Please note that possible cyber-attacks cannot be fully avoided by the below mentioned recommendations and set of measures already performed by ComAp, but by following them the cyber-attacks can be considerably reduced and thereby to reduce the risk of damage. ComAp does not take any responsibility for the actions of persons responsible for cyber-attacks, nor for any damage caused by the cyber-attack. However, ComAp is prepared to provide technical support to resolve problems arising from such actions, including but not limited to restoring settings prior to the cyber-attacks, backing up data, recommending other preventive measures against any further attacks.

Warning: Some forms of technical support may be provided against payment. There is no legal or factual entitlement for technical services provided in connection to resolving problems arising from cyber-attack or other unauthorized accesses to ComAp's Products or Services.

- The controller web interface at port TCP/80 is based on http, not https, and thus it is intended to be used only in closed private network infrastructures.
- Avoid exposing the port TCP/80 to the public Internet.

Support

For further support, please, contact your local ComAp representative. For contact information, see https://www.comap-control.com/contact-us/comap-worldwide.

ComAp Disclaimer

This document was created by the ComAp and only ComAp may change the document at any time in its sole discretion.

ComAp hereby disclaims any liability for the accuracy, quality, security, completeness, functionality, or other aspect of any information contained of this document (“Content”). ComAp shall have no responsibility or liability for any errors or omissions in the Content.

THE CONTENT IS PROVIDED „AS-IS“ WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE

WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND/OR AGAINST INFRINGEMENT.

COMAP SHALL UNDER NO CIRCUMSTANCES BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF CONTRACTS, LOSS OF OPPORTUNITY, LOSS OF BUSINESS, LOSS OR DEPLETION OF GOODWILL, INCREASED OVERHEADS OR ADMINISTRATION EXPENSES, MANAGEMENT TIME, LOSS OF SAVINGS, LOSS OF DATA OR ANY TYPE OF SPECIAL, INDIRECT OR CONSEQUENTIAL LOSS OF ANY NATURE WHATSOEVER (INCLUDING WITHOUT LIMITATION LOSS OR DAMAGE SUFFERED BY YOU AS A RESULT OF AN ACTION BROUGHT BY ANY THIRD PARTY) EVEN IF SUCH LOSS WAS REASONABLY FORESEEABLE OR COMAP HAD BEEN ADVISED OF THE POSSIBILITY OF YOU INCURRING THAT LOSS WHETHER UNDER THIS DOCUMENT OR OTHERWISE.

This document and any of its parts hereof may not be reproduced, modified, altered, combined, in any way without written permission from ComAp, and the Contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.