1 Advisory Information

- **Advisory ID:** BOSCH-SA-538331-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2020-6776
    - Base Score: 8.8 (High)
  - CVE-2020-6777
    - Base Score: 4.8 (Medium)
  - CVE-2020-15688
    - Base Score: 7.5 (High)
- **Published:** 30 Sep 2020
- **Last Updated:** 30 Sep 2020

2 Summary

Two security vulnerabilities have been uncovered in the web based management interface of the PRAESIDEO Network Controller and the PRAESENSA System Controller. The vulnerabilities will allow a Cross-Site Request Forgery (CSRF) attack and a Cross-site Scripting (XSS) attack.

For PRAESIDEO a third vulnerability will allow a replay attack with which authentication can be bypassed. This last vulnerability is present in the web server of the PRAESIDEO Network Controller.

All hardware revisions of the PRAESIDEO Network Controller and the PRAESENSA System Controller are affected by these vulnerabilities. Unfortunately patching is not available for some older (out of service) models of the PRAESIDEO Network Controller. Further details are provided in the Solution and Mitigations section.

The vulnerabilities in PRAESIDEO have been discovered and responsibly disclosed by the external researcher Gjoko Krstic.

3 Affected Products

- Bosch PRAESENSA <= 1.10
  - CVE-2020-6776
  - CVE-2020-6777
- Bosch PRAESIDEO
  - CVE-2020-15688
- Bosch PRAESIDEO <= 4.41
  - CVE-2020-6776
  - CVE-2020-6777

4 Solution and Mitigations

4.1 Software Updates

The recommended approach is to update the software of the affected Bosch product to the following or later releases: for PRAESIDEO version 4.42 and for PRAESENSA version 1.20.

Please note that for PRAESIDEO the LBB4401/00 and PRS-NCO-B Network Controllers (both of which have reached End of Service) do not support the 4.42 release due to technical limitations. We recommend to apply the mitigation measures described below.

4.2 Isolate the system

For PRAESIDEO the recommendation that is already made in the user manual is repeated: it is strongly advised to run PRAESIDEO on an isolated network that is not connected to a public network. Isolating will significantly reduce the odds of having an attacker misuse the vulnerabilities. Note that for the LBB4401/00 and PRS-NCO-B Network Controllers (both of which have reached End of Service) this mitigation will be the only solution since they do not support the 4.42 release due to technical limitations.

The PRAESIDEO user manual contains the following caution:

> "The PRAESIDEO network interfaces do not provide extensive security measures to protect the system against malicious network attacks. Such measures would be insufficient on the long term anyway, because PRAESIDEO systems in operation are unlikely to be updated regularly to repair security leaks. Therefore do not keep the network controller permanently connected to an open Ethernet network. When a network connection is needed after configuration, e.g. in case of connection to a PC Call Server or a Logging Server, then use a separate network, not accessible by others, or setup a PRAESIDEO specific VLAN by using Ethernet switches with VLAN capabilities to partition the network into multiple broadcast domains with one domain assigned solely to PRAESIDEO."

For PRAESENSA we refer to the general security whitepaper of which the steps are also documented in the installation manual. The most important recommendation with respect to these vulnerabilities is:

> "It is highly recommended to operate PRAESENSA on its own dedicated network, not mixed with other equipment for other purposes. Other equipment may be accessible by unauthorized people, causing a security risk. This is especially true if the network is connected to the Internet."

4.3 Firewalling (network)

In case the system for some reason must be connected to a public network it is strongly advised to firewall the PRAESIDEO or PRAESENSA system. Firewalling the PRAESIDEO and PRAESENSA systems significantly reduces the attack surface. It is advised not to enable port-forwarding to the PRAESIDEO Network Controller or the PRAESENSA System Controller since that will revert the reduction of the attack surface.

5 Vulnerability Details

5.1 CVE-2020-6776

CVE description: A vulnerability in the web-based management interface of Bosch PRAESIDEO until and including version 4.41 and Bosch PRAESENSA until and including version 1.10 allows an unauthenticated remote attacker

to trigger actions on an affected system on behalf of another user (Cross-Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or submitting a malicious form. A successful exploit allows the attacker to perform arbitrary actions with the privileges of the victim, e.g. creating and modifying user accounts, changing system configuration settings and cause DoS conditions.

Note: For Bosch PRAESIDEO 4.31 and newer and Bosch PRAESENSA in all versions, the confidentiality impact is considered low because user credentials are not shown in the web interface.

- Problem Type:
  - CWE-352 Cross-Site Request Forgery (CSRF)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

5.2 CVE-2020-6777

CVE description: A vulnerability in the web-based management interface of Bosch PRAESIDEO until and including version 4.41 and Bosch PRAESENSA until and including version 1.10 allows an authenticated remote attacker with admin privileges to mount a stored Cross-Site-Scripting (XSS) attack against another user. When the victim logs into the management interface, the stored script code is executed in the context of his browser. A successful exploit would allow an attacker to interact with the management interface with the privileges of the victim. However, as the attacker already needs admin privileges, there is no additional impact on the management interface itself.

- Problem Type:
  - CWE-79 Cross-site Scripting (XSS)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
  - Base Score: 4.8 (Medium)

5.3 CVE-2020-15688

The GoAhead webserver used in Bosch PRAESIDEO does not protect against replay attacks on HTTP Digest Authentication. For PRAESIDEO 4.31 and later, a possible HTTP Digest Authentication capture-replay is limited to 300 seconds (i.e. an attacker must capture and replay within 5 minutes after an authenticated user uses the PRAESIDEO web interface to have the attack succeed). We suggest customers to apply the mitigations described in this advisory since the PRAESIDEO web server does not support TLS/HTTPS.

CVE description: The HTTP Digest Authentication in the GoAhead web server before 5.1.2 does not completely protect against replay attacks. This allows an unauthenticated remote attacker to bypass authentication via capture-replay if TLS is not used to protect the underlying communication channel.

- Problem Type:
  - CWE-294 Authentication Bypass by Capture-replay
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 7.5 (High)

5.4 Remark

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

6 Additional Resources

- [1] PRAESIDEO Network Controller Downloads: https://commerce.boschsecurity.com/us/en/Network-controller/F.01U.249.771/
- [2] PRAESENSA System Controller Downloads: https://commerce.boschsecurity.com/us/en/PRAESENSA-Public-Address-and-Voice-Alarm-System/p/64306699275/

Please contact the Bosch PSIRT if you have feedback, comments, or additional information about this vulnerability at: psirt@bosch.com.

7 Revision History

- 30 Sep 2020: Initial Publication

8 Appendix

8.1 Material List: Bosch PRAESIDEO

SAP Number	CTN	Description
F.01U.506.857	LBB4401/00	Network Controller – End of Service reached
F.01U.126.533	PRS-NCO-B	Network Controller – End of Service reached
F.01U.249.771	PRS-NCO3	Network Controller
F.01U.318.441	PRS-NCO3-CN	网络控制器 (Network Controller)

8.2 Material List: Bosch PRAESENSA

SAP Number	CTN	Description
F.01U.325.042	PRA-SCL	System controller, large