Cyber Security Advisory Hasplms vulnerabilities in PCM600 and SAB600

ABBVU-EPDS-B41769

Update Date: *if updated*

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, 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.

Affected Products

SAB600 3.5

SAB600 3.5.1

PCM600 2.4

PCM600 2.4.0.1

PCM600 2.4.0.2

PCM600 2.4.1

PCM600 2.4.1.1

PCM600 2.4.1.2

PCM600 2.4.1.3

Vulnerability ID

ABB ID:	ABBVU-EPDS-B41769
CVE ID:	CVE-2017-11498, CVE-2017-11497, CVE-2017-11496

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above.

An unauthenticated attacker who successfully exploited this vulnerability could cause the product to cause a remote process crash or execute arbitrary code on remote system.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both CVSS v2 and v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v3 Base Score:	7.5 (High)
CVSS v3 Temporal Score:	6.7 (Medium)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v3 Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

NVD Summary Link:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11498
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11497
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11496

Corrective Action or Resolution

The problem is corrected in the following product versions:

- PCM600 2.5 or later
- SAB600 4.0 or later

ABB recommends that customers apply the update at the earliest convenience.

Vulnerability Details

A vulnerability exists in the Sentinel HASP Run-time Environment (hasplms service) included in the product versions listed above. An attacker could exploit the vulnerability by uploading a specially crafted file to the service creating a buffer overflow. Buffer overflows may allow remote attackers to execute arbitrary code or to shut down the remote process (a denial of service).

Mitigating Factors

Updates that remove the affected components are available. ABB recommends that customers apply the update at the earliest convenience.

Frequently asked questions

What is the scope of the vulnerability?

The exploit may allow remote attackers to execute arbitrary code or to shut down the remote process (a denial of service). An attacker who successfully exploited this vulnerability could prevent legitimate access to PCM600 and SAB600.

What is the hasplms?

Hasplms is a license service management component. Licenses were used to enable or disable PCM600 and SAB600 functionality in the affected versions. The need for licenses was removed in subsequent releases.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted file and uploading it to Gemalto ACC (Admin Control Center). This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or has local access to the vulnerable node.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?

The update removes the service from installation. The service is not used in corrected products.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, this vulnerability has been publicly disclosed.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?
No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

- Vladimir Dashchenko of Kaspersky Labs

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.