ABB DOC ID: 1MRS257783
REVISION: A
DATE: 2018-06-28

CYBER SECURITY ADVISORY

Sentinel HASP/LDK License Manager Vulnerabilities in MicroSCADA Pro SYS600 9.2, 9.3, 9.4

ABBVU-PGGA-36052

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.

Affected Products

MicroSCADA Pro SYS600 9.2, 9.3, 9.4

Vulnerability ID

ABB ID: ABBVU-PGGA-36052

CVE ID: CVE-2017-11498, CVE-2017-11497, CVE-2017-11496, CVE-2017-12818, CVE-2017-12819, CVE-2017-12820, CVE-2017-12821, CVE-2017-12822

Summary

ABB is aware of public reports of a vulnerability in the Gemalto Sentinel HASP/LDK License Manager software, which is used in MicroSCADA Pro SYS600 9.2, 9.3 and 9.4.

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

In addition, Microsoft has documented a known issue (reboot loop) with old Sentinel HASP drivers when deploying Microsoft security updates/rollups of March 2018 and following rollups, see link. ABB has confirmed reboot loop issues with at least Windows 7 and Windows Server 2008 SP2 machines. It is recommended to follow instructions in this advisory to install Sentinel HASP/LDK 7.80 version with latest drivers before deploying Microsoft security updates.

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: 9.9 (Critical)

CVSS v3 Temporal Score: 9.5 (Critical)

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L/E:H/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:C/C:H/I:L/A:L/E:H/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
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12818
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12819
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12820
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12821
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12822

Recommended immediate actions

The problem is fixed by Gemalto in the following product version:

- Sentinel HASP/LDK License Manager version 7.80

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

The update is supported in following operating systems: Windows 7 SP1, Windows 8.1 SP1, Windows Server 2008 R2 SP1, Windows Server 2012 R2, Windows Server 2016, Windows 10 Version 1709. Other and older operating system versions are likely to be fully compatible as well, but Gemalto does not guarantee this. Outside above mentioned operating systems ABB has tested the update in Windows Server 2008 SP2.

Download and Installation Instructions

1. The update can be downloaded from Gemalto/Sentinel download page and selecting *Sentinel HASP/LDK – Command Line Run-time Installer, Version 7.80, Released 2018-04-12* installation package. Extract the zip file.
2. Stop MicroSCADA service from SYS600 Control Panel
3. Stop hasplms service by opening Command Prompt window (run as admin) and running command 'sc stop hasplms'. After stopping the service, run command 'sc query hasplms' to verify that the service is stopped.
4. Run 'haspdinst.exe -info' to check what driver versions are installed to the system and versions included in the installation package.
5. Run 'haspdinst.exe -purge' to uninstall old Sentinel HASP component versions
6. Run 'haspdinst.exe –install' to install the Sentinel HASP 7.80 version. Note that in some machines e.g. Windows Server 2008 SP2 you might see few times 'Windows can't verify the publisher of this driver software' messages where you should answer 'Install this driver software anyway'.
7. After the installation is finished, **reboot the machine.**
8. After the reboot, start MicroSCADA service from SYS600 Control Panel and verify that there are no hardware license key related error messages in SYS600 Notify window.

Important note: After the installation, hasplms service is started automatically and there is a Windows Firewall rule named "Sentinel License Manager".

To enhance security, it is recommended to block all traffic to hasplms service (TCP and UDP 1947) since this service is not needed to be accessed remotely in SYS600 systems. Modify the firewall rule in Windows Firewall inbound rules and configure it to block traffic to hasplms service. If there are duplicate firewall rules regarding hasplms.exe and TCP/UDP 1947, delete duplicates.

If a hardware license key is not used in SYS600 system or by any other software, then hasplms service can be disabled completely by running commands in Command Prompt:

1. sc stop hasplms
2. sc config hasplms start=disabled

If needed, the service can be re-enabled using following commands:

1. sc config hasplms start=auto
2. sc start hasplms

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

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, 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, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

More information on recommended practices can be found in the ICS-CERT documents.

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 SYS600.

What is the hasplms?

Hasplms is a license management component. In SYS600, Hasplms is used when the license is attached to a hardware license key (USB dongle).

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 fixes the vulnerabilities.

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.

My system does not use a hardware license key (USB dongle). Is it ok to uninstall Sentinel HASP License Manager?

ABB recommends to install the update as instructed in this advisory and then disable hasplms service by running following commands in the Command Prompt window:

1. sc stop hasplms
2. sc config hasplms start=disabled

Note that future SYS600 installation packages may contain updated Sentinel HASP version, which again starts hasplms service. It is required to manually disable hasplms service again.

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 https://new.abb.com/contact-centers.

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