GE Digital Product Security Communication

Title:	Gemalto HASP Driver Vulnerabilities
Vulnerability ID:	GED SecComm 18-02
Communication Release date:	05 01 2018
Last Updated:	05 09 2018

Summary

Multiple vulnerabilities have been identified in the 3rd party service provided to GE Common Licensing by Gemalto Inc.

All reported findings are addressed in GE Digital Common Licensing v18.3released April 2018.

Details identified by Kaspersky Labs ICS Cert in early 2017 can be found in the link below. In late 2016 and early 2017, 11 vulnerabilities were identified. In June 2017 three more vulnerabilities were discovered.

https://ics-cert.kaspersky.com/alerts/2017/10/03/several-more-vulnerabilities-found-and-closed-in-popular-license-manager/

> *"Kaspersky Lab ICS CERT has identified multiple vulnerabilities: denial of service (DOS), NTLM-relay attack, Stack buffer overflow, Remotely enabling web admin interface, Arbitrary memory read and possible remote code execution (RCE) in hasplms service that is a part of Gemalto's HASP SRM, Sentinel HASP and Sentinel LDK products."*

Kaspersky Labs generated the CVE documents below. The CVSS v3 Base Scores can be viewed on each CVE and range from a low of 7.3 to a high of 10.0.

- CVE-2017-11496 – Remote Code Execution
- CVE-2017-11497 – Remote Code Execution
- CVE-2017-11498 – Denial of Service
- CVE-2017-12818 – Denial of Service
- CVE-2017-12819 – NTLM hash capturing
- CVE-2017-12820 – Denial of Service
- CVE-2017-12821 – Remote Code Execution
- CVE-2017- 12822 – Remote manipulations with configuration files

Visit Gemalto's security bulletins for more information (pages are restricted and log in is required to view the content.)

https://sentinel.gemalto.com/technical-support/security-updates-sm/

https://supportportal.gemalto.com/csm/?id=csm_product&sys_id=50303b92db852e00d298728dae96199d&table=sn_customerservice_product_name (in this page please the **"Security Bulletins"** section).

Affected software

GE Common Licensing v18.2 and prior

Solution

GE Common Licensing version 18.3 released April 2018 contains mitigations for Kaspersky Lab's findings. GE recommends users ensure they are using the latest version of Common Licensing.

To obtain the latest versions of this product please contact your local GE Digital representative. Contact information is available at https://digitalsupport.ge.com/communities/CC_Contact

Other Recommendations

GE Digital recommends that all customers upgrade to the latest GE Common Licensing version 18.3. Other recommendations may mitigate issues but only installing the most current version will fully address an issue.

Firewall Policy - Review corporate firewall policies. The reported vulnerabilities do not apply if port 1947 is blocked by firewall.

Sentinel LDK License Manager - For users not using USB keys, it is possible to turn off the service that is affected by the findings outlined above. If possible, turn off the *Sentinel LDK License Manager* service.

Disclaimer

Product communications provided here are subject to terms and conditions contained in customers' underlying license agreements or other applicable agreements. Due to ongoing product enhancements, GE reserves the right to change or update communications without advance notification.

Auto-Notification

Please visit the customer profile page on the support site to sign up for auto-notifications for GE Digital products to receive immediate notice of security alerts and information.

Instructions on "How to sign up for Auto-Notifications for updates" can be found here;

https://digitalsupport.ge.com/communities/en_US/Article/How-to-sign-up-for-SIM-Auto-Notification-for-GE-Intelligent-Platforms-software-products-KB12680-en-US

Change log

Date	Change(s)
May 1, 2018	Initial release
May 9, 2018	Vulnerability ID, Affected Software version, Other Recommendations