Security Bulletin

Bulletin Number
[160318]

Issue Date
11 Apr 2018

CVE
CVE-2018-8900

Severity Level
Medium

Products Affected
All versions of hasplms ranging from HASP SRM, Sentinel HASP, Sentinel LDK v2.10 – v7.66

Known Exploits
None

Mitigation Provided

Update Run-Time Environment for LDK to version 7.80

Sentinel License Manager Vulnerabilities

Description

The License Manager service of HASP SRM, Sentinel HASP and Sentinel LDK products prior to Sentinel LDK RTE 7.80, is affected under following scenario:

> Remote attackers can inject malicious web script in the logs page of Admin Control Center (ACC) for cross-site scripting (XSS) vulnerability.

Risk Assessment

An attacker can exploit this attack to deface the log page in ACC and to redirect users. The confidentiality and integrity of the files on the target system may be compromised if the vulnerability is exploited.

Mitigation Strategies

Customers who have Sentinel LDK (RTE) Run-time Environment version (v2.10 –7.66) are advised to update their Sentinel LDK RTE to the latest Sentinel LDK RTE component (v7.80). This update can be found on the Sentinel Downloads site.

Customer Support

https://supportportal.gemalto.com/

Gemalto acknowledges Niv Levy (an information security consultant / penetration tester from Israel) for responsible disclosure of these vulnerabilities.

[End of Bulletin]