Security Bulletin

Bulletin Number
[20170616_1]

Issue Date
16 June 2017

CVE
N/A

Severity Level
Medium

Products Affected
All versions of hasplms ACC (Admin Control Center) ranging from HASP SRM 2.10 to Sentinel LDK 7.50.

Known Exploits
None

Mitigation Provided
Update Run-Time Environment for LDK to version 7.55

Sentinel License Manager Vulnerabilities

Description

In Jan 2017, Kaspersky shared 11 python scripts to exhibit the attacks on Sentinel LDK License Manager service. These attacks are categorized in the 3 issues in Sentinel LDK License Manager service. Post investigation, it was concluded that, the License Manager service of HASP SRM, Sentinel HASP and Sentinel LDK products, prior to Sentinel LDK RTE 7.55 were affected by this vulnerability. The scenarios were:

1) Language pack (ZIP file) with invalid HTML files lead to NULL pointer access. Hacker can create language pack file on their own with invalid HTML file. The vulnerability can be exploited for denial of service.
2) Language packs containing filenames longer than 1024 characters lead to a stack buffer overflow. The vulnerability can be exploited for an arbitrary code execution.
3) Malformed ASN1 streams in V2C and similar input files can be used to generate stack buffer overflows. The vulnerability can be exploited for an arbitrary code execution.

The service is vulnerable in the default configuration, but it can be configured to require an authentication with password to access the Admin interface that allows this attack.

Risk Assessment

The Sentinel LDK License Manager service runs with administrative privileges. The confidentiality and integrity of the files on the target system may be compromised if the vulnerability is exploited.

Denial of service attack could result in non-availability of the Sentinel LDK License Manager service. This may impact licensed application relying on the license manager service.

Mitigation Strategies

Customers who have Sentinel LDK (RTE) Run-time Environment version (v2.10 – 7.50) are advised to update their Sentinel LDK RTE to the latest Sentinel LDK RTE

component (v 7.55) which was released on May 25, 2017. This update can be found on the Sentinel Downloads site.

Customer Support

https://supportportal.gemalto.com/csm

Gemalto acknowledges Kaspersky for responsible disclosure of these vulnerabilities.

[End of Bulletin]