ICS-CERT ADVISORY

ICSA-11-314-01—SAFENET SENTINEL AND 7T IGSS INPUT SANITIZATION VULNERABILITY

December 12, 2011

OVERVIEW

ICS-CERT originally released advisory ICSA-11-314-01P on the US-CERT secure portal on November 14, 2011. This web page release was delayed to allow users time to download and install the update.

Security researcher Carlos Mario Penagos Hollman of Synapse-labs[a] has identified an input sanitization vulnerability in SafeNet Sentinel HASP Software Rights Management (HASP-SRM) license management application.

ICS-CERT has coordinated the researcher's vulnerability report with SafeNet, and SafeNet has produced an updated version that mitigates this vulnerability. Mr. Penagos has tested the updated version and validates that it resolves the vulnerability.

AFFECTED PRODUCTS

The following products are affected:

- SafeNet Sentinel HASP SDK releases older than Version 5.11
- Sentinel HASP Run-time installers older than Version 6.x
- 7 Technologies (7T) IGSS Version 7.

IMPACT

Successful exploitation of this vulnerability allows an attacker to change the code in a configuration file. Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

SafeNet is a US-based company that creates products for software protection and license management. The affected products, Sentinel HASP, formerly Aladdin HASP SRM, are the digital license manager keys used to enforce digital licenses that enable the use of software or hardware. According to SafeNet, these products are used worldwide.

a. http://synapse-labs.com/EN/node, website last accessed December 12, 2011.

7T IGSS uses the SafeNet Sentinel HASP SDK for its digital license manager to enable its software products.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The web application Sentinel HASP Admin Control Center, which is accessed remotely, does not sufficiently validate user input. This characteristic can allow attackers to craft and inject HTML code into the configuration file.

The vulnerability can be reproduced using Mozilla Firefox 2.0. As of this writing (November 2011), it is not reproducible with the current versions of Mozilla Firefox, Microsoft Internet Explorer, Opera, and Google Chrome.

CVE-2011-3339[b] has been assigned to this vulnerability. SafeNet calculated a CVSS v2 base score of 4.3 and an overall score of 0.9 for this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

Exploiting this vulnerability requires a moderate skill set.

MITIGATION

SafeNet has provided the following links to allow users to download an updated version that mitigates this vulnerability:

http://www3.safenet-inc.com/support/hasp-srm/enduser.aspx#Runtime

http://www3.safenet-inc.com/support/hasp-srm/vendor.aspx#latestDD .

SafeNet has also provided more information regarding this vulnerability as well as installation instructions for the updated version at the following location:

http://www.safenet-inc.com/support-downloads/sentinel-drivers/CVE-2011-3339/.

b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3339. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

In addition to upgrading the SafeNet software, ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control system security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[c] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

May I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public websites. All comments or questions related to this document should be directed to ICS-CERT at ics-cert@dhs.gov.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before

c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed December 12, 2011.

public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.