View more Gemalto solutions (http://www.gemalto.com)

Security Vulnerability in Sentinel HASP® Run-time Environment v.5.95 and Earlier

Dec. 12, 2011

This document provides the solution from SafeNet, Inc. for the vulnerability described in ICS-CERT Advisory ICSA-11-314-01, which was issued by the U.S. Department of Homeland Security.

Overview

ICS-CERT Advisory ICSA-11-314-01 describes a vulnerability that was found in Sentinel HASP Admin Control Center, one of the components of Sentinel HASP Run-time Environment. As a result of this vulnerability, it may be possible for a malicious user to inject HTML code into the Admin Control Center configuration file.

This vulnerability would only expose users who match *both* of the following criteria:

- The user is working with **Sentinel HASP Run-time Environment v.5.95 or earlier**.

  AND

- The user is working with Sentinel HASP Admin Control Center in **Mozilla Firefox version 2.0**.

  As of the time of writing, the vulnerability has not been found to be reproducible with the current versions of Mozilla Firefox, Microsoft Internet Explorer, Opera and Google Chrome

To date, no known exploitations of this vulnerability have been found in the wild.

The vendor-assigned overall CVSS score for this vulnerability is 0.9. This score represents a very low risk to users of SafeNet Sentinel Admin Control Center. The score is based on the combination of the vulnerability Base score with Environmental Score Metrics (for example, very small user base for Firefox 2.0), as well as Temporal Score Metrics (availability of an Official Fix from SafeNet).

SafeNet Inc. acknowledges that this vulnerability exists and has released an updated Run-time Environment installer that eliminates the vulnerability. The procedure for downloading and installing the updated Run-time Environment is described below.

Installing the Updated Run-time Environment

Users of Sentinel HASP Admin Control Center can download and install an updated version of Sentinel HASP Run-time Environment that eliminates the reported vulnerability.

To download the updated Run-time Environment installer:

Go to this address:
http://www3.safenet-inc.com/support/hasp-srm/enduser.aspx#Runtime (http://www3.safenet-inc.com/support/hasp-srm/enduser.aspx#Runtime)

Download and save the file: **Sentinel_HASP_Run-time_ setup.zip**

To install the updated Run-time Environment:

1. Unzip the file Sentinel_HASP_Run-time_ setup.zip (that you downloaded in the previous procedure) into a temporary directory.
2. Close all applications that require a Sentinel HASP (hardware or software) protection key.
3. In the temporary directory, double-click the file HASPUserSetup.exe.
4. Follow the instructions displayed by the installation wizard, accepting all default responses.

Note: To install the Run-time Environment, you require administrator access rights on your computer. Under Vista and Windows 7, you may be required to enter the password for a user with administrator rights.

The full text of the original ICS-CERT Advisory can be found at this location:

http://www.us-cert.gov/control_systems/pdf/ICSA-11-314-01.pdf (http://www.us-cert.gov/control_systems/pdf/ICSA-11-314-01.pdf)

Copyright © 2011 SafeNet, Inc. All rights reserved.

1. Try searching our website:

Search Data Protection

GO

By continuing your visit, you accept the use of cookies. Find out more. (/privacy-statement/) Hide Me

Search Sentinel

GO

Security Vulnerability in Sentinel HASP® Run-time Environment v.5.95 and Earlier

Dec. 12, 2011

This document provides the solution from SafeNet, Inc. for the vulnerability described in ICS-CERT Advisory ICSA-11-314-01, which was issued by the U.S. Department of Homeland Security.

Overview

ICS-CERT Advisory ICSA-11-314-01 describes a vulnerability that was found in Sentinel HASP Admin Control Center, one of the components of Sentinel HASP Run-time Environment. As a result of this vulnerability, it may be possible for a malicious user to inject HTML code into the Admin Control Center configuration file.

This vulnerability would only expose users who match *both* of the following criteria:

- The user is working with **Sentinel HASP Run-time Environment v.5.95 or earlier**.

  AND

- The user is working with Sentinel HASP Admin Control Center in **Mozilla Firefox version 2.0**.

  As of the time of writing, the vulnerability has not been found to be reproducible with the current versions of Mozilla Firefox, Microsoft Internet Explorer, Opera and Google Chrome

To date, no known exploitations of this vulnerability have been found in the wild.

The vendor-assigned overall CVSS score for this vulnerability is 0.9. This score represents a very low risk to users of SafeNet Sentinel Admin Control Center. The score is based on the combination of the vulnerability Base score with Environmental Score Metrics (for example, very small user base for Firefox 2.0), as well as Temporal Score Metrics (availability of an Official Fix from SafeNet).

SafeNet Inc. acknowledges that this vulnerability exists and has released an updated Run-time Environment installer that eliminates the vulnerability. The procedure for downloading and installing the updated Run-time Environment is described below.

Installing the Updated Run-time Environment

Users of Sentinel HASP Admin Control Center can download and install an updated version of Sentinel HASP Run-time Environment that eliminates the reported vulnerability.

To download the updated Run-time Environment installer:

Go to this address:
http://www3.safenet-inc.com/support/hasp-srm/enduser.aspx#Runtime (http://www3.safenet-inc.com/support/hasp-srm/enduser.aspx#Runtime)

Download and save the file: **Sentinel_HASP_Run-time_ setup.zip**

To install the updated Run-time Environment:

1. Unzip the file Sentinel_HASP_Run-time_ setup.zip (that you downloaded in the previous procedure) into a temporary directory.
2. Close all applications that require a Sentinel HASP (hardware or software) protection key.
3. In the temporary directory, double-click the file HASPUserSetup.exe.
4. Follow the instructions displayed by the installation wizard, accepting all default responses.

Note: To install the Run-time Environment, you require administrator access rights on your computer. Under Vista and Windows 7, you may be required to enter the password for a user with administrator rights.

The full text of the original ICS-CERT Advisory can be found at this location:

http://www.us-cert.gov/control_systems/pdf/ICSA-11-314-01.pdf (http://www.us-cert.gov/control_systems/pdf/ICSA-11-314-01.pdf)

Copyright © 2011 SafeNet, Inc. All rights reserved.

Privacy Policy (http://www.gemalto.com/companyinfo/privacy-policy) | EU Commitments (http://www.gemalto.com/companyinfo/about/merger/commitments) | Sitemap (/complete-products-list/) | Disclaimer (http://www.gemalto.com/companyinfo/disclaimer) | Terms & Conditions (/terms-conditions/) | © 2006- 2017 Gemalto NV