Document: Identity Engines “Heartbleed” Response

Version: 1.0

Published date: 10 Apr 2014

Updated: 10 Apr 2014

Author: Shmulik Nehama

DETAILS

An issue has been reported via CVE (Common Vulnerabilities and Exposures) with open-source OpenSSL that, if exploited, can lead to exposure of sensitive system data on affected products.

PROBLEM CLARIFICATION

Further information on the CVE-2014-0160 can be found at http://heartbleed.com and https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160.

CAUSE

Identity Engines Release 8.x and below are not impact by this security vulnerability.

Identity Engines Ignition Server Release 9.0 is impacted by this security vulnerability. Other Identity Engines Release 9.0 applications (such as the Dashboard, Guest Manager, CASE Manager, Access Portal and Analytics) are not impacted by this security vulnerability. Identity Engines Release 9.0 was released a few days before the CVE-2014-0160 OpenSSL Heartbleed Vulnerability became public information.

While Avaya does not have any reports of this exploit being used in the wild, advanced notice of this is being provided.

SOLUTION

Avaya will be issuing an Identity Engines Release 9.0.1 for the Ignition Server and Dashboard (for compatibility considerations) on the Avaya PLDS web site as soon as it is available. Expected timeframe is by April 30th or before.

For protection in the intermediate time, customers are advised NOT to enable SSH on the Ignition Server and NOT to apply the SSO license.

In addition, note that since the Ignition Server is typically deployed within the enterprise datacenter, the exposure to this security vulnerability is reduced and applies only to Ignition Server Release 9.0.