OpenSSL Heartbleed Vulnerability in Relion 650 series Ver. 1.3.0
ABB-VU-PSAC-1MRG016162

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Copyright © 2014 ABB. All rights reserved.

Affected Products
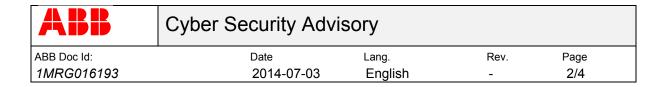
Relion 650 series Ver. 1.3.0

Summary

A vulnerability has recently been published that affects certain versions of OpenSSL and is commonly referred to as "Heartbleed". The vulnerability also affects the product versions listed above.

Additional Information can be found here:

- http://www.kb.cert.org/vuls/id/720951

- https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-099-01B

If an attacker successfully exploits this vulnerability, it could cause unauthorized disclosure of information from the product. In particular, the vulnerability allows an attacker to search for usernames and passwords in the product.

Severity rating

The severity rating for this vulnerability is important, with the overall CVSS score 5. This assessment is based on the types of systems that are affected by the vulnerability, how difficult it is to exploit, and the effect that a successful attack exploiting the vulnerability could have.

CVSS Overall Score: 4.8

CVSS Vector: *(AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:W/RC:C)*

CVSS Link:
http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:W/RC:C)

Corrective Action or Resolution

ABB has investigated this vulnerability and have now released a maintenance release in order to provide adequate protection to customers. ABB have issued a maintenance release for the 650 series Ver. 1.3.0 that will fix this issue, 650 series Ver. 1.3.0.1.

Based on the customers risk assessment and exposure of the system, the maintenance release should be applied.

If user-defined accounts have been used, the passwords of those should be changed. It is also advised that cryptographic keys are re-generated by temporarily changing IP-address or IEC61850 name of the device.

ABB recommends that customers also follow the steps outline in the section "Mitigating Factors".

Customers shall contact their local ABB contacts to obtain the maintenance release.

Vulnerability Details

A vulnerability exists in OpenSSL included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, allowing the attacker to get unauthorized disclosure of information from the product.

Mitigating Factors

Recommended security practices and firewall configurations can help protect an industrial control network from attacks that originate from outside the network. Such practices include that industrial control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Industrial control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and

removable storage media should be carefully scanned for viruses before they are connected to a control system.

Workarounds

Workarounds are described in the *Corrective Action or Resolution* chapter above.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploits this vulnerability could get hold of the user credentials and cryptographic keys used to login to the device.

What causes the vulnerability?
The vulnerability is caused by a bug in OpenSSL 1.0.1c that is used in the 650 series Ver. 1.3.0.

What is the affected product or component?
In the Relion 650 series Ver. 1.3.0, the affected parts are the FTPS protocol and the tool access protocol. Both protocols uses the OpenSSL component.

What might an attacker use the vulnerability to do?
An attacker who successfully exploits this vulnerability could get hold of the user credentials and cryptographic keys used to access the device.

How could an attacker exploit the vulnerability?
An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?
Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that industrial control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

When this security advisory was issued, had this vulnerability been publicly disclosed?
Yes, this vulnerability has been publicly disclosed.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited in the 650 series Ver. 1.3.0 when this security advisory was originally issued.

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com/substationautomation.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.