Welcome IP-Gateway Command Injection, Missing Session Management and Clear Text Passwords in Cookies ABB-VU-EPBP-R-2505

Update Date:
2018-05-14 original document
2018-06-05 details clarified

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.

Affected Products

IP-Gateway is available under two brands:

- ABB
- Busch-Jaeger

Busch-Jaeger Elektro GmbH is part of the ABB Group.

IP-Gateway – ABB-Welcome System Device (Article No.: 83342-500), Version: 3.39 and all prior versions

IP-Gateway – Busch-Jaeger Systemgerät (Article No.: 83342), Version: 3.39 and all prior versions

Vulnerability ID

ABB ID:	ABB-VU-EPBP-R-2505
CVE ID:	CVE-2017-7931, CVE-2017-7933, CVE-2017-7906
ICS-CERT ID:	ICS-VU-281953

Summary

An update is available that resolves a privately reported vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could take remote control of the product and run arbitrary code.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for CVSS v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v3 Base Score:	9,6 (Critical)
CVSS v3 Temporal Score:	8,6
CVSS v3 Vector/Link:	AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:X

Corrective Action or Resolution

The problem is corrected in the following product versions:

IP-Gateway (ABB-Welcome System Device and Busch-Jaeger Systemgerät) firmware version 3.40. However, customers are advised to update their devices to version 3.48 or later.

ABB recommends that customers apply the update at earliest convenience. The SW is available for download at the product page of the Busch-Jaeger catalogue in section Software:

- http://www.busch-jaeger-catalogue.com/artikel.php?bereich=1016301&programm=1016477&gruppe=1016493&produkt=1016494
- http://www.busch-jaeger-katalog.de/artikel.php?bereich=1016301&programm=1016477&gruppe=1016493&produkt=1016494

Vulnerability Details

There are multiple vulnerabilities which are described in detail below.

Remote code injection

A remote code injection vulnerability exists in the IP-Gateways' local configuration webserver included in the affected product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system allowing the attacker to take control of the product or insert and run arbitrary code. The attacker must have direct network access to the affected IP-Gateway in order to exploit this vulnerability.

Improper authentication (CVE-2017-7931)

Missing session management made it possible for a malicious user to be able to access the configuration files and application pages without authentication.

Plaintext storage of a password (CVE-2017-7933)

It is possible to read administrators password from the cookie in a users browser after successful login. The attacker must first compromise the client system in order to successfully extract the clear-text password cookie.

Cross-site request forgery (CVE-2017-7906)

The product is vulnerable to cross-site request forgery attacks. The web server does not sufficiently verify that a request was performed by the authenticated user. This may allow for an attacker to launch a request impersonating that user.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a network from attacks that originate from outside the network. Such practices include that 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.

Workarounds

ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as "Impact of workaround".

The affected products configuration website shall not be reachable from the internet. Any existing direct internet connection, e.g., port forwarding on a router, shall be disabled.

Accessing the IP-Gateway's local configuration webserver in a browser's anonymous/incognito mode assures deletion of the clear-text password cookie after the browser tab or window is closed. Hence, minimizing the amount of time an attacker has the ability to exploit this vulnerability.

Furthermore it is important to access the IP-Gateway’s local configuration webserver exclusively within the local network and not over the Internet as the IPGW does not support a TLS protected connection (HTTPS). In case a customer demands accessing the configuration webserver remotely, a VPN connection to the IP-Gateway’s local network is recommended.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could take control of an affected system node or insert and run arbitrary code in an affected system node.

What causes the vulnerability?
The vulnerability is a mix of missing session management and unchecked input in the IP-Gateway local webserver configuration.

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 direct network access to an affected product could exploit this vulnerability.

No, if the affected product is installed according to the products security disclaimer, the vulnerability can’t be exploited remotely. Recommended practices include that systems are physically protected, have no option to be connected from the Internet but can itself connect to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?
The update removes the vulnerabilities by modifying the way that the IP-Gateway validates messages and by introducing a session management.

When this security advisory was issued, had this vulnerability been publicly disclosed?
No, ABB received information about this vulnerability through responsible disclosure.

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 when this security advisory was originally issued.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

- Florian Grunow of ERNW GmbH for responsibly disclosing the aforementioned vulnerabilities.
- Maxim Rupp for responsibly disclosing the aforementioned vulnerabilities.
- ICS-CERT for coordinating this vulnerability.

Support

For additional information and support please contact your local ABB service organization.

Please contact info.bje@de.abb.com or find more information at www.busch-jaeger.de for ABB and Busch-Jaeger.

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