DOCUMENT ID: 2PAA121232
REVISION: D
DATE: 2020-06-09

CYBERSECURITY ADVISORY

SECURITY System 800xA Information Manager - Remote Code Execution

CVE ID: CVE-2020-8477

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

System 800xA, Information Manager — Versions 5.1, 6.0 (6.0.0 to 6.0.3.3) and 6.1

Vulnerability IDs, Product Issue Numbers

CVE ID	Product Issue Numbers
CVE-2020-8477	800xAINM-OL-5101-016

Summary

ABB is aware that the Information Manager for System 800xA contains a Remote Code Execution vulnerability which require user attention. An attacker who successfully exploited this vulnerability could insert and run arbitrary code on an Information Manager node (client or server).

Vulnerability severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (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:	8.8 (High)
CVSS v3 Temporal Score:	8.1 (High)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
NVD Summary Link:	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8477

Recommended immediate actions

The vulnerability is corrected in Information Manager 5.1 Rev E/5.1 FP4 Rev E TC6.
ABB recommends customers on the 800xA 5.1 track to install this TC. This TC can be obtained from technical support on request.

This vulnerability is corrected in Information Manager 6.0.3.3 RU1.
ABB recommends customers on the 800xA 6.0.3 LTS track to update to System 800xA version 6.0.3.3 and to install RU1 for IM.

The vulnerability is corrected in Information Manager 6.1 RU1.
ABB recommends customers on the 800xA 6.1 track to install this roll up.

The above-mentioned updates are recommended regardless of whether the previously described manual removal of the vulnerable component has been done or not. The IM rollups for 6.0.3.3 and 6.1 can be downloaded from My ABB/My Control System.

Please note that the vulnerability can be exploited by Remote and Unauthenticated users, so customers are recommended to ensure that only authorized persons have access to plant assets and network and that web browsing from system nodes to external networks is restricted, especially from an IM node.

Check that the usage of the Access Enable key in AC 800M HI and the configured access level of SIL variables corresponds to the risk analysis. See the FAQ “Can functional safety be affected by an exploit of this vulnerability?” below.

Vulnerability details

An attacker who successfully exploited the vulnerability in the IM node (client or server), will be able to run arbitrary code. Successful exploitation of this vulnerability requires luring a user (on a host with the vulnerable IM component installed) to access a malicious website, that instructs the user’s browser to load the vulnerable component, before passing it malicious input.

This could cause the Display Services functionality to stop, but it could also cause other system functionality to stop or to malfunction.

Mitigating factors

Successful exploitation of this vulnerability requires luring a user to a malicious website, so the primary mitigation is to restrict web browsing from IM nodes to external networks, e.g. by blocking this in a network firewall.

Recommended baseline security practices and firewall configurations can help protect a network and its attached devices from attacks that originate from outside the network. For example, common practices are for process control systems to be 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 must be evaluated case by case.

Process control and automation systems should not be used for general business functions (e,g. internet browsing, email, etc.) which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Recommended practices include that process 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.

Workarounds

No work arounds exist. Please refer the “Recommended Immediate Actions” Section.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could execute arbitrary code in the IM server.

What causes the vulnerability?

This is caused due to a component in 800xA Information Manager which does not properly validate input data. Moreover, this component should not have been included in the product delivery.

What is the Information Manager?

Information Management functionality includes History Services for collection, online and offline storage, consolidation, and retrieval for process/lab data, alarms/events, and reports.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could execute arbitrary code.

Can functional safety be affected by an exploit of this vulnerability?

Under certain conditions exploits of this vulnerability may affect the integrity of safety functions in System 800xA. This is however prevented if the Access Enable key in the AC 800M HI is turned Off ("disabled") and Access Level for the variables in the safety applications are configured to "Read Only" or "Confirm and Access Enable" (see *3BNP004865* AC 800M High Integrity Safety Manual* for more information regarding SIL Access Control and Confirmed Write Support).
With other configurations exploits of this vulnerability may affect the integrity of safety functions in System 800xA. This risk is then best avoided by following the advice in section "Recommended immediate actions" above.
It can be noted that creating malware that exploits this vulnerability and affects the integrity of a safety function will involve a substantial amount of intricate reverse engineering to circumvent the existing safety measures in AC 800M HI.

How could an attacker exploit the vulnerability?

An attacker could try to exploit this vulnerability by luring a user (on a host with the vulnerable IM component installed) to access a malicious website, that instructs the user's browser to load the vulnerable component, before passing it malicious input.

Could the vulnerability be exploited remotely?

Yes, an attacker that manages to lure a user to navigate to a remote webserver with malicious content could exploit this vulnerability.

What does the update do?

The Information Manager rollups 6.0.3.3 RU1 and 6.1 RU1 removes the vulnerable component which is not needed by the product. Information Manager 5.1 Rev E/5.1 FP4 Rev E TC6 replaces the vulnerable component with a non-vulnerable component.

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

Acknowledgement

ABB thanks William Knowles at Applied Risk for helping to identify the vulnerabilities and protecting our customers.

Support

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

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

Revisions

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2020-03-30
B	P4 all	Added FAQ question on functional safety Misc clarifications	2020-04-17
C	P2,3,4	Updated "Recommended Immediate Actions" and added "What does the update do?" due to correction released in System 800xA 6.0.3.3	2020-05-14
D	Recommended immediate actions, all	Describing the 5.1 Rev E/5.1 FP4 Rev E TC6, 6.0.3.3 RU1 and 6.1 RU1. Generalized the scope to both IM Clients and IM Servers	2020-06-09