Security Advisory

SAV-0001 : Deserialization of untrusted data in fdtCONTAINER component and fdtCONTAINER application

Date published:	Planned for 2021-01-11
Version	V1.1
Last update	2020-12-08
Severity	High
CVE	CVE-2020-12525

Vulnerability 1 Deserialization of untrusted data in fdtCONTAINER component
CWE-502: Deserialization of untrusted data
CVSSv3.1 base score 7.3
AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C

Vulnerability 2 Deserialization of untrusted data in fdtCONTAINER application
CWE-502: Deserialization of untrusted data
CVSSv3.1 base score 7.3
AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C

Aditional References

None

Description

The fdtCONTAINER component is integrated into an application (host application).
The fdtCONTAINER application is a specific host application which integrates the fdtCONTAINER component.

The fdtCONTAINER component exchanges binary data blobs with such a host application. Typically, the host application saves these binary data blobs into a project storage (project file or a project database).
To manipulate the data inside the project storage, the attacker needs write access to this project storage. Additionally, the manipulated project needs to be opened by the host application. It depends on the host application whether opening the project requires a user action or not. In fdtCONTAINER applications, the user has to open the manipulated project file manually.

In the case of opening a stored project, the deserialization of the manipulated data can be exploited.

Impact

The engineering workstation, on which the host application is executed, might execute malicious code with the user rights of the host application.

Security Advisory

Affected Products

fdtCONTAINER component

Affected versions	Fixed versions
3.5.0 - <3.5.20304.x	3.5.20304.x
3.6.0 - <3.6.20304.x	3.6.20304.x
< 3.5	Not available

fdtCONTAINER application

Affected versions	Fixed versions
4.5.0 - <4.5.20304.x	4.5.20304.x
4.6.0 - <4.6.20304.x	4.6.20304.x
< 4.5	Not available

dtmINSPECTOR

Affected Version	Fixed versions
3 (Based on FDT 1.2.x)	Available in Q1/2021

dtmINSPECTOR is a specific fdtCONTAINER application. The following information about the fdtCONTAINER application also applies.

Solution

Update the fdtCONTAINER component / fdtCONTAINER application to a version that provides a more secure deserialization of the project data. This version will still use a deprecated serialization technology, but will fix the currently known attack vector and will be compatible with existing, non-manipulated project files.

Update the fdtCONTAINER component / fdtCONTAINER application to a version that provides a secure deserialization of the project data with an updated serialization technology. This will break the compatibility to existing, non-manipulated project files.

Mitigation

1. Exchange project data only via secure exchange services
2. Use appropriate means to protect the project storage from unauthorized manipulation
3. Do not open project data from an unknown source
4. Reduce the user rights of the host application to the necessary minimum

Additional Resources

None

Reported

Reported by a customer of the fdtCONTAINER component.

Disclaimer

The security instructions given here have exclusively technical-informatory character; contractual relationships are not established by this; existing contractual stipulations remain unaffected.

https://www.mm-software.com/de/agbs

In case of any questions please contact psirt@mm-software.com.