TOMTEC Imaging Systems GmbH
Freisinger Str. 9, 85716 Unterschleissheim, Germany

UNTERSCHLEISSHEIM,
17.05.2021

Vulnerability Disclosure Information 2021-0001

Dear Valued Customer,

Following a responsible disclosure process to continuously maintain the security of our products, we would like to inform you about some minor vulnerabilities within our software that we have become aware of.

CVE-2019-12741

This vulnerability, reported in the "National Vulnerability Database" database (https://nvd.nist.gov/), concerns a third-party software which is integrated into **TOMTEC-ARENA TTA2.3x.xx**. You can find information about which version of TOMTEC-ARENA you are using in the About Box dialog.

Who is affected?

You could be affected, if you are using TOMTEC-ARENA within an unsecure environment (e.g. it is not protected from unauthorized access physically or remotely by using for example an up-to-date firewall or any other means).

How can this vulnerability affect you?

In case someone gets access (remote or physically) to your network and is able to directly inject malicious code into the TOMTEC-ARENA front end or uses social engineering techniques to mislead a user into opening a malicious link on the machine TOMTEC-ARENA is installed on, the attacker could gain unauthorized access to TOMTEC-ARENA.

What can I do if I am not protected?

The vulnerability has already been fixed with TOMTEC-ARENA TTA2.40.00. Thus, an update to **TOMTEC-ARENA TTA2.40.00 (or later)** will resolve this vulnerability.

In general you should always run TOMTEC-ARENA on a secure system with exclusive access rights for authorized staff. Furthermore your staff should be aware of the general security risk when opening links or attachments provided by uncertain sources.

TOMTEC Imaging Systems GmbH
Freisinger Str. 9
85716 Unterschleissheim
Deutschland/Germany

o +49 89 32175 500
f +49 89 32175 750
e info@tomtec.de
w www.tomtec.de

Amtsger. München: HRB 235646
Managing Director: Matthijs Groot Wassink, Dr. Thomas Piehler
Tax Number: 27/278/00002
USt-Id-Number: DE 813013647

CVE-2020-8112

This vulnerability, reported in the "National Vulnerability Database" database (https://nvd.nist.gov/), concerns a third-party software which is integrated into **TOMTEC-ARENA TTA2.31.xx, TOMTEC-ARENA TTA2.40.xx and TOMTEC-ARENA TTA2.41.xx**. You can find information about which version of TOMTEC-ARENA you are using in the About Box dialog.

Who is affected?

You could be affected, if you are using TOMTEC-ARENA within an unsecure environment (e.g. it is not protected from unauthorized access physically or remotely by using for example an up-to-date firewall or any other means).

How can this vulnerability affect you?

In case someone gets access (remote or physically) to your network and is able to send a manipulated JPEG contained in a DICOM file to TOMTEC-ARENA, the attacker could cause a buffer overflow that may result in leakage of sensitive information.

What can I do if I am not protected?

You should always run TOMTEC-ARENA on a secure system with exclusive access rights for authorized staff only to prevent anyone from being able to send manipulated DICOM files within your network.

The vulnerability will be fixed with **TOMTEC-ARENA TTA2.42.00 (or later)**, scheduled to be released end of July 2021.

CVE-2020-17510

This vulnerability, reported in the "National Vulnerability Database" database (https://nvd.nist.gov/), concerns a third-party software which is integrated into **TOMTEC-ARENA TTA2.31.xx, TOMTEC-ARENA TTA2.40.xx and TOMTEC-ARENA TTA2.41.xx**. You can find information about which version of TOMTEC-ARENA you are using in the About Box dialog.

Who is affected?

You could be affected, if your server running TOMTEC-ARENA is used within an unsecure environment (e.g. it is not protected from unauthorized access physically or remotely by using for example an up-to-date firewall or any other means).

How can this vulnerability affect you?

In case someone gets access (remote or physically) to your network, the person could send a manipulated http request to the TOMTEC-ARENA server that may lead to the acquisition of unauthorized access to TOMTEC-ARENA.

What can I do if I am not protected?

You should always run TOMTEC-ARENA on a secure system with exclusive access rights for authorized staff only.

The vulnerability will be fixed with **TOMTEC-ARENA TTA2.42.00 (or later)**, scheduled to be released end of July 2021.

Please contact TOMTEC Service & Support (support@tomtec.de) in case you have questions or wish an update.

Kind regards

GREGOR MALISCHNIG
CMO