TagMaster

LEARN FROM REALITY

Approved by	Issued By	Date	Document ID.	Revision
TagMaster PSIRT	TagMaster PSIRT	2020-12-08	**1120-213**	07

Security Advisory: NuttX TCP/IP vulnerabilities – AMNESIA:33

Overview

Initial release date	2020-12-08
Current release date	2020-12-08
CVE ID(s)	CVE-2020-17437
Affected products	XT-1, XT Mini (all firmware versions prior to 1.6.8)
Status	Resolved for all affected products

Revision History

Revision	Date	Issued by	Comment
07	2020-12-08	TagMaster PSIRT	Initial public release

TagMaster

LEARN FROM REALITY

Approved by	Issued By	Date	Document ID.	Revision
TagMaster PSIRT	TagMaster PSIRT	2020-12-08	**1120-213**	07

CVE-2020-17437

Description

The vulnerability, which is a part of the vulnerabilities commonly referred to as AMNIESA:33, affects the network stack such that an attacker could set up an invalid data pointer for TCP packet data, by setting the urgent flag and manipulating the value of the urgent pointer to a value beyond the size of the packet itself.

CWE	CWE-125
CVSS	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H (8,2)
Affected products	XT-1, XT Mini
Affected FW-versions	All prior to 1.6.8
Status	Resolved in firmware release 1.6.8

Resolution

The CVE has been patched and will be released (in firmware version 1.6.8) by the 8th of December 2020. Contact TagMaster support for details on how to obtain and install the latest firmware version.

Acknowledgements

Jos Wetzels, Amine Amri, Stanislav Dashevskyi and Daniel dos Santos at Forescout Technologies
BSI
CISA

Miscellaneous

In general has the process for Cybersecurity at TagMaster been updated during October 2020, and the email address of cybersecurity@tagmaster.com and the corresponding public PGP key will be published on the company web page.

This security advisory is published at:
https://tagmaster.com/wp-content/uploads/2020/12/1120-213-Security-Advisory-NuttX-TCP-IP-vulnerabilities.pdf