CRA SAMPLE

F05 Vulnerability ticket

Example after one year of operation, status 05.02.2028 · Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect

Publisher	OT-Cyber.de, Max Gilg, Rosenheim
Sample company	Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect (fictitious)
Note	Free sample, not legal advice

Company, people, data and numbers are fictitious. This is how the document looks after one year of operation.

1 Purpose and scope

One ticket per vulnerability covering triage, safety relevance, deadline, remediation and closure (P07). If the vulnerability is actively exploited, the notification under Article 14 CRA (F06) is also required.

2 Document control

Field	Entry
Document no.	NWT-CE-F05
Version, status	1.7, approved
Scope	NWT HACKTHERM 60 connect (18 to 60 kW), controller, gateway, portal and app
Author	Jonas Weiß, Engineering and Product Security (PSO)
Checked by	Ingenieurbüro Lechner (safety), Sichtwerk Security (security)
Approval	Michael Berger, Managing Director, 05.02.2028
Next review	15.03.2029 or in the event of a substantial modification
Confidentiality	internal
Filing	Technical documentation NWT-TD-HT60C, retained for at least 10 years after the last unit is placed on the market

3 Vulnerability ticket: overview

Ticket	Component	CVSS	Active	Deadline	Fixed
NWT-VULN-2027-001	Gateway kernel	5.5	no	90 days	20.05.2027
NWT-VULN-2027-002	Controller (manufacturer advisory)	6.1	no	90 days	05.09.2027
NWT-VULN-2027-003	Portal, guessable user name	5.3	no	90 days	12.06.2027
NWT-VULN-2027-004	MQTT library	7.1	no	30 days	26.06.2027
NWT-VULN-2027-005	App, library	4.3	no	90 days	20.11.2027
NWT-VULN-2027-006	Portal component	8.8	yes	7 days	16.10.2027
NWT-VULN-2028-001	Gateway, TLS setting	5.9	no	90 days	14.02.2028

Legend: CVSS = severity score from 0 to 10.

4 In detail: NWT-VULN-2027-004

Received: 14.06.2027, 09:12, advisory from the MQTT library project

Affected: MQTT library in the gateway up to and including firmware 1.4.1

Assessment: Memory error triggered by manipulated messages; exploitation requires control of the broker; CVSS 7.1

Safety relevance: No: the gateway has no access to F-data (fail-safe data) (D07 C04)

Actively exploited: No, checked on 14.06.2027 and daily until closure

Remediation: Library updated, firmware 1.4.2 (NWT-REL-142), rollout 24.06. 1 %, 26.06. 100 %

User information: Security advisory NWT-SA-2027-002

Closure: 28.06.2027, J. Weiß, daily monitoring of the library

5 Terms and abbreviations

CRA: Cyber Resilience Act, Regulation (EU) 2024/2847

CVSS: severity score of a vulnerability from 0 to 10

MQTT: messaging protocol between device and portal

NWT: abbreviation of the sample company in document and ticket numbers

REL: release, an approved software version (number range)

SA: security advisory to users (number range)

TLS: encryption of the connection

VULN: vulnerability ticket (number range)

6 Revision history and approval

Version	Date	Change	Approval
1.0	15.03.2027	Register opened	M. Berger
1.2	23.05.2027	NWT-VULN-2027-003	M. Berger
1.3	28.06.2027	NWT-VULN-2027-004	M. Berger
1.5	30.10.2027	NWT-VULN-2027-006	M. Berger
1.7	05.02.2028	NWT-VULN-2028-001	M. Berger

Approved: Michael Berger, Managing Director, 05.02.2028 (signed in the original). Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.