CRA SAMPLE

F07 Security advisory to users

Example after one year of operation, status 28.02.2028 · 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

Published security advisories with content, channel and date (Annex I, Part II, points (4) and (8), Article 14(8)). Each advisory states what happened, who is affected and what the user should do.

2 Document control

Field	Entry
Document no.	NWT-CE-F07
Version, status	1.5, 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, 28.02.2028
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 Security advisory to users: overview

Advisory	Date	Topic	Severity	Affected, fixed	User must
NWT-SA-2027-001	12.06.2027	Portal: user name guessable	medium, 5.3	Portal up to 2027.06.0, fixed in 2027.06.1	nothing
NWT-SA-2027-002	26.06.2027	Gateway: MQTT library	high, 7.1	Gateway up to 1.4.1, fixed in 1.4.2	nothing, automatic update
NWT-SA-2027-003	16.10.2027	Portal: actively exploited vulnerability	high, 8.8	Portal up to 2027.10.1, fixed in 2027.10.2	password change recommended
NWT-SA-2028-001	14.02.2028	Gateway: TLS setting	medium, 5.9	Gateway up to 1.5.0, fixed in 1.5.1	nothing, automatic update

4 Content of NWT-SA-2027-003

What happened: attackers attempted to exploit a vulnerability in a component of our portal. Severity: high (CVSS 8.8). Affected: portal up to version 2027.10.1, fixed in 2027.10.2.

Who is affected: all portal accounts; your heating system and its safety functions were not affected.

What we did: closed the vulnerability on 16.10.2027, reviewed the logs and found no successful access.

What you should do: change your portal password if you also use it elsewhere. MFA remains active.

Contact: psirt@nordwald-waerme.example

Channels: Portal (home page and inbox), email to all operator accounts, app notification where action is required

Deadlines: together with the update; for actively exploited vulnerabilities, no later than the notification under Article 14

Mandatory content: Description, affected versions, impact, severity and remediation (Annex I, Part II, point (4)); added for all advisories in the table since 28.02.2028

Archive: all advisories publicly available at nordwald-waerme.example/security, at least until the end of the support period

5 Terms and abbreviations

CVSS: severity score of a vulnerability from 0 to 10

MFA: multi-factor authentication

MQTT: messaging protocol between device and portal

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

SA: security advisory to users (number range)

TLS: encryption of the connection

6 Revision history and approval

Version	Date	Change	Approval
1.0	15.03.2027	Template introduced	M. Berger
1.1	12.06.2027	NWT-SA-2027-001	M. Berger
1.2	26.06.2027	NWT-SA-2027-002	M. Berger
1.3	16.10.2027	NWT-SA-2027-003	M. Berger
1.4	14.02.2028	NWT-SA-2028-001	M. Berger
1.5	28.02.2028	Severity and affected versions per advisory	M. Berger

Approved: Michael Berger, Managing Director, 28.02.2028 (signed in the original). Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.