CRA SAMPLE

F06 Reporting record under Article 14 CRA

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

Records every notification submitted to the single reporting platform, including time, content and reference. Example: an actively exploited vulnerability in a portal component in October 2027.

2 Document control

Field	Entry
Document no.	NWT-CE-F06
Version, status	1.4, 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 Reporting record under Article 14 CRA: overview

Awareness: 14.10.2027, 07:40: notice from Sichtwerk that attacks on the component had been observed on the internet; exploitation attempts also found in our portal logs

Affected: Portal (remote data processing) up to version 2027.10.1; boiler and controller not affected

Immediate measures: 08:20 web application firewall rule deployed against the attack pattern; 09:00 maintenance authorisations suspended

Classification: Actively exploited within the meaning of Article 3(42) CRA: on 14.10.2027 the component manufacturer confirmed successful exploitation at other operators; in our case only attempts occurred. Notification obligation therefore confirmed

Recipient: BSI as coordinating CSIRT (main establishment in Germany), via the ENISA single reporting platform; platform case number in file F06-2027-01

Component manufacturer: Informed of our own observations on 14.10.2027 at 09:30 (Article 13(6) CRA); patch confirmed on 15.10.2027

Step	Deadline	Sent	Reference
Early warning	15.10.2027, 07:40	14.10.2027, 10:05	in file F06-2027-01

Step	Deadline	Sent	Reference
Notification	17.10.2027, 07:40	16.10.2027, 14:30	in file F06-2027-01
Final report	14 days after remediation	29.10.2027	in file F06-2027-01

Notification content: Type of vulnerability (authentication bypass in a web component), observed exploitation attempts, no successful login, remediation through version 2027.10.2 on 16.10.2027, severity high

User information: NWT-SA-2027-003 on 16.10.2027 in the portal and by email to all operators

Outcome: Log analysis: no successful access; safety functions were not affected at any time (D07, limits in the F section)

4 Terms and abbreviations

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

CSIRT: national computer security incident response team, receives the reports

ENISA: EU Agency for Cybersecurity, runs the single reporting platform under the CRA

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

SA: security advisory to users (number range)

VULN: vulnerability ticket (number range)

5 Revision history and approval

Version	Date	Change	Approval
1.0	15.03.2027	Form introduced	M. Berger
1.1	28.09.2027	Notification exercise	M. Berger
1.2	17.10.2027	Notification NWT-VULN-2027-006	M. Berger
1.3	30.10.2027	Final report	M. Berger
1.4	28.02.2028	Classification, recipient and notification to the component manufacturer added	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.