CRA-MUSTER

F05 Schwachstellentickets

Beispiel nach einem Jahr Betrieb, Stand 05.02.2028 · Nordwald Wärmetechnik GmbH, vernetzter Hackgutkessel NWT HACKTHERM 60 connect

Herausgeber	OT-Cyber.de, Max Gilg, Rosenheim
Musterbetrieb	Nordwald Wärmetechnik GmbH, vernetzter Hackgutkessel NWT HACKTHERM 60 connect (frei erfunden)
Hinweis	Kostenfreies Muster, keine Rechtsberatung

Firma, Personen, Daten und Nummern sind frei erfunden. So sieht das Dokument nach einem Jahr gelebtem Betrieb aus.

1 Zweck und Geltungsbereich

Ein Ticket je Schwachstelle mit Triage, Safety-Bezug, Frist, Maßnahme und Abschluss (P07). Bei aktiver Ausnutzung zusätzlich die Meldung nach Art. 14 (F06).

2 Dokumentenlenkung

Feld	Eintrag
Dokument-Nr.	NWT-CE-F05
Version, Status	1.7, freigegeben
Geltungsbereich	NWT HACKTHERM 60 connect (18 bis 60 kW), Steuerung, Gateway, Portal und App
Ersteller	Jonas Weiß, Technik und Product Security (PSO)
Geprüft	Ingenieurbüro Lechner (Safety), Sichtwerk Security (Security)
Freigabe	Michael Berger, Geschäftsführer, 05.02.2028
Nächste Prüfung	15.03.2029 oder bei wesentlicher Änderung
Vertraulichkeit	intern
Ablage	Technische Dokumentation NWT-TD-HT60C, aufbewahrt bis mindestens 10 Jahre nach Inverkehrbringen der letzten Einheit

3 Schwachstellentickets

Ticket	Komponente	CVSS	Aktiv	Frist	Behoben
NWT-VULN-2027-001	Gateway-Kernel	5.5	nein	90 Tage	20.05.2027
NWT-VULN-2027-002	Steuerung (Hersteller-Advisory)	6.1	nein	90 Tage	05.09.2027
NWT-VULN-2027-003	Portal, Benutzername erratbar	5.3	nein	90 Tage	12.06.2027
NWT-VULN-2027-004	MQTT-Bibliothek	7.1	nein	30 Tage	26.06.2027
NWT-VULN-2027-005	App, Bibliothek	4.3	nein	90 Tage	20.11.2027
NWT-VULN-2027-006	Portal-Komponente	8.8	ja	7 Tage	16.10.2027
NWT-VULN-2028-001	Gateway, TLS-Einstellung	5.9	nein	90 Tage	14.02.2028

Legende: CVSS = Schweregrad einer Schwachstelle von 0 bis 10; Aktiv = aktiv ausgenutzt.

4 Ausführlich: NWT-VULN-2027-004

Eingang: 14.06.2027, 09:12, Advisory des Projekts der MQTT-Bibliothek

Betroffen: MQTT-Bibliothek im Gateway bis Firmware 1.4.1

Bewertung: Speicherfehler bei manipulierten Nachrichten, Ausnutzung setzt Kontrolle über den Broker voraus; CVSS 7.1

Safety-Bezug: nein: Gateway hat keinen Zugriff auf F-Daten (D07 C04)

Aktiv ausgenutzt: nein, geprüft am 14.06.2027 und täglich bis zum Abschluss

Maßnahme: Bibliothek aktualisiert, Firmware 1.4.2 (NWT-REL-142), Rollout 24.06. 1 %, 26.06. 100 %

Nutzerinformation: Sicherheitshinweis NWT-SA-2027-002

Abschluss: 28.06.2027, J. Weiß, Monitoring der Bibliothek täglich

5 Begriffe und Abkürzungen

CVSS: Schweregrad einer Schwachstelle von 0 bis 10

MQTT: Nachrichtenprotokoll zwischen Gerät und Portal

NWT: Kürzel des Musterbetriebs in Dokument- und Ticketnummern

REL: Release, also ein freigegebener Softwarestand (Nummernkreis)

SA: Sicherheitshinweis an Nutzer (Nummernkreis)

TLS: Verschlüsselung der Verbindung

VULN: Schwachstellenticket (Nummernkreis)

6 Änderungshistorie und Freigabe

Version	Datum	Änderung	Freigabe
1.0	15.03.2027	Register eröffnet	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

Freigegeben: Michael Berger, Geschäftsführer, 05.02.2028 (im Original unterschrieben). Kostenfreies Muster von OT-Cyber.de, keine Rechtsberatung. Firma, Personen, Seriennummern und Daten frei erfunden.