Richtlinie zur koordinierten Offenlegung von Sicherheitslücken (CVD)

LANTECH Informationstechnik GmbH

63930 Klingenberg am Main / Deutschland

Version: 1.0
Gültig ab: 08.09.2026
Letzte Aktualisierung: 08.09.2026

1. Zweck

Die LANTECH Informationstechnik GmbH („LANTECH“) legt großen Wert auf die Sicherheit ihrer Produkte und den Schutz ihrer Kunden, Nutzer und Partner.

Diese Richtlinie zur koordinierten Offenlegung von Sicherheitslücken (Coordinated Vulnerability Disclosure, CVD) legt einen strukturierten Prozess fest, nach dem Sicherheitsforscher, Kunden, Partner und andere Parteien potenzielle Sicherheitslücken melden können, die LANTECH Produkte betreffen.

LANTECH fördert eine verantwortungsvolle und koordinierte Offenlegung, damit gemeldete Sicherheitslücken untersucht, bewertet und behoben werden können, bevor detaillierte Informationen öffentlich bekannt gegeben werden.

2. Geltungsbereich

Diese Richtlinie gilt für Sicherheitslücken, die in Produkten mit digitalen Komponenten identifiziert werden, die von LANTECH hergestellt werden, einschließlich, soweit zutreffend:

- Hardwareprodukte;
- eingebettete Software und Firmware;
- Produktbetriebssysteme;
- webbasierte Verwaltungsschnittstellen;
- webbasierte Anwendungen;
- Software-Tools und -Anwendungen;
- mit LANTECH-Produkten gelieferte Software;

Für Produkte, deren Supportzeitraum abgelaufen ist, besteht möglicherweise nur eingeschränkter oder gar kein Support für Sicherheitsupdates. LANTECH wird dennoch Meldungen zu solchen Produkten prüfen und auf der Grundlage des damit verbundenen Cybersicherheitsrisikos geeignete Maßnahmen festlegen. Der Begriff „Produkte“ umfasst sowohl Hardware- als auch Softwareprodukte.

3. Meldung einer Sicherheitslücke

Mögliche Sicherheitslücken sollten über den folgenden Sicherheitskontakt an LANTECH gemeldet werden:

Globale Sicherheitskontaktstelle: cra@lantech-group.eu
Sicherheits-Website: https://www.lantech.eu/cra

Bitte verwenden Sie folgende Betreffzeile:

Sicherheitslücken-Meldung – [Produktname]

Damit LANTECH das Problem effizient untersuchen kann, geben Sie bitte so viele der folgenden Informationen wie möglich an:

- Name und Modell/Version des betroffenen Produkts;
- Hardware-Revision, falls zutreffend;
- Firmware- oder Softwareversion;
- detaillierte Beschreibung der Sicherheitslücke;
- Schritte zur Reproduktion des Problems;
- mögliche Auswirkungen auf die Sicherheit;
- Proof-of-Concept-Informationen, Screenshots, Protokolle oder andere relevante Nachweise;
- bekannte Ausnutzungsbedingungen;
- Vorschläge zur Risikominderung oder Behebung, sofern vorhanden;
- Ihre bevorzugten Kontaktdaten;
- ob Sie öffentlich genannt werden möchten.

Bitte geben Sie keine sensiblen personenbezogenen Daten an, es sei denn, dies ist für die Untersuchung erforderlich.

4. Was Sie von LANTECH erwarten können

Nach Erhalt einer Sicherheitslücke wird LANTECH angemessene Anstrengungen unternehmen, um:

1. den Eingang des Berichts zu bestätigen;
2. die Informationen zu prüfen und festzustellen, ob das gemeldete Problem reproduzierbar ist;
3. die potenziellen Auswirkungen auf die Cybersicherheit und den Schweregrad zu bewerten;
4. mit dem Melder zu kommunizieren, falls zusätzliche Informationen erforderlich sind;
5. bei Bedarf geeignete Abhilfemaßnahmen oder Maßnahmen zur Risikominderung zu entwickeln;
6. Sicherheitsupdates gemäß den geltenden Richtlinien zum Produktsupport bereitstellen;
7. die Offenlegung der Sicherheitslücke gegebenenfalls koordinieren; und
8. veröffentlichen bei Bedarf relevante Sicherheitsinformationen oder einen Sicherheitshinweis.

Die zur Behebung einer Sicherheitslücke benötigte Zeit hängt von deren Komplexität, Schweregrad, den betroffenen Produkten, der Verfügbarkeit von Abhilfemaßnahmen und der Notwendigkeit der Abstimmung mit Drittanbietern von Komponenten ab.

5. Koordinierte Offenlegung

LANTECH bittet Melder, eine angemessene Frist für die Untersuchung und Behebung einzuräumen, bevor detaillierte Informationen über eine gemeldete Sicherheitslücke öffentlich bekannt gegeben werden.

Während der Untersuchung werden die Melder gebeten:

- die Details der Sicherheitslücke vertraulich zu behandeln, bis die koordinierte Offenlegung erfolgt ist;
- die Veröffentlichung von Exploit-Code oder technischen Informationen zu vermeiden, die eine böswillige Ausnutzung erleichtern könnten, bevor eine Behebung oder Abmilderung verfügbar ist;
- Vermeiden Sie den Zugriff auf, die Änderung, das Löschen oder die Entwendung von Daten, die anderen Parteien gehören;
- Handlungen zu vermeiden, die Produktionssysteme oder -dienste stören könnten;
- keine Denial-of-Service-Tests an Betriebssystemen durchzuführen, sofern dies nicht ausdrücklich genehmigt wurde; und
- mit LANTECH bei der Festlegung eines angemessenen Zeitplans für die Offenlegung zusammenzuarbeiten.

LANTECH wird sich bemühen, die Offenlegung mit dem Melder und, sofern relevant, mit betroffenen Lieferanten, Komponentenherstellern, Wartungsunternehmen, CSIRTs oder anderen zuständigen Behörden abzustimmen.

6. Bewertung und Behebung von Sicherheitslücken

Gemeldete Schwachstellen werden anhand ihrer technischen Merkmale und des damit verbundenen Cybersicherheitsrisikos bewertet.

Gegebenenfalls kann LANTECH anerkannte Methoden zur Schwachstellenbewertung, einschließlich des Common Vulnerability Scoring System (CVSS), zur Unterstützung der Einstufung des Schweregrads heranziehen.

Je nach Bewertung kann die Behebung Folgendes umfassen:

- Firmware- oder Software-Updates;
- Konfigurationsänderungen;
- ausgleichende Sicherheitsmaßnahmen;
- vorübergehende Abhilfemaßnahmen;
- Aktualisierungen der Produktdokumentation;
- Sicherheitshinweise; oder
- andere geeignete Korrekturmaßnahmen.

Betrifft eine Sicherheitslücke eine in ein LANTECH-Produkt integrierte Komponente eines Drittanbieters, kann LANTECH sich mit dem jeweiligen Hersteller, Lieferanten oder Betreuer dieser Komponente abstimmen.

7. Sicherheitsupdates und -hinweise

Werden Sicherheitsupdates bereitgestellt, stellt LANTECH den betroffenen Nutzern entsprechende Informationen zur Verfügung, damit diese das betroffene Produkt identifizieren und die erforderlichen Abhilfemaßnahmen oder Maßnahmen zur Risikominderung ergreifen können.

Sicherheitshinweise können gegebenenfalls Folgendes umfassen:

- betroffene Produktmodelle;
- betroffene Firmware- oder Softwareversionen;
- Beschreibung der Sicherheitslücke;
- Auswirkungen auf die Sicherheit;
- Einschätzung des Schweregrads;
- CVE-Kennung, sofern zutreffend;
- behobene Versionen;
- verfügbare Abhilfemaßnahmen oder Workarounds; und
- Anweisungen zum Abrufen und Installieren des Sicherheitsupdates.

In begründeten Fällen können detaillierte Informationen zur Sicherheitslücke vorübergehend zurückgehalten werden, wenn eine sofortige Veröffentlichung das Cybersicherheitsrisiko erhöhen könnte, bevor betroffene Nutzer eine angemessene Gelegenheit hatten, die entsprechenden Abhilfemaßnahmen anzuwenden.

8. Verantwortungsvolle Sicherheitsforschung

LANTECH begrüßt in gutem Glauben durchgeführte Sicherheitsforschung, die darauf abzielt, die Cybersicherheit seiner Produkte zu verbessern.

Forscher sollten ihre Aktivitäten verantwortungsbewusst und in Übereinstimmung mit den geltenden Gesetzen sowie dieser Richtlinie durchführen.

Sicherheitstests sollten sich auf Systeme und Produkte beschränken, die sich im Besitz des Forschers befinden oder für die der Forscher eine entsprechende Genehmigung eingeholt hat.

Forscher dürfen nicht vorsätzlich:

- die Privatsphäre oder Sicherheit anderer Nutzer gefährden;
- auf Daten zugreifen, die über das zur Demonstration einer Schwachstelle erforderliche Maß hinausgehen;
- Daten Dritter verändern oder löschen;
- Malware einschleusen;
- Dienste oder Betriebsnetzwerke stören;
- Social-Engineering-Angriffe gegen Mitarbeiter, Kunden oder Partner von LANTECH durchführen; oder
- entdeckte Schwachstellen für rechtswidrige Zwecke nutzen.

9. Anerkennung

Gegebenenfalls und mit Zustimmung des Meldenden kann LANTECH Personen oder Organisationen würdigen, die gültige Sicherheitslücken verantwortungsbewusst melden.

Jede öffentliche Würdigung wird vor der Veröffentlichung mit dem Melder abgestimmt.

10. Meldung an Aufsichtsbehörden

Soweit dies nach den geltenden Cybersicherheitsvorschriften erforderlich ist, kann LANTECH Schwachstellen, Vorfälle oder damit zusammenhängende Informationen an zuständige Behörden, Computer Security Incident Response Teams (CSIRTs), die ENISA oder andere benannte Stellen melden.

Solche Meldepflichten gegenüber Aufsichtsbehörden sind unabhängig von dem in dieser Richtlinie beschriebenen koordinierten Verfahren zur Offenlegung von Sicherheitslücken.

11. Kontakt

Fragen zu dieser Richtlinie oder Meldungen potenzieller Schwachstellen sind zu richten an:

LANTECH Informationstechnik GmbH
Philipp-Kachel-Str. 42a
63911 Klingenberg / Deutschland

Ansprechpartner für globale Sicherheit: cra@lantech-group.eu
Globale Sicherheits-Website: https://www.lantech.eu/cra

Bitte fügen Sie bei Sicherheitslückenmeldungen ausreichende technische Informationen bei, damit LANTECH das gemeldete Problem reproduzieren und bewerten kann.

12. Aktualisierungen der Richtlinie

LANTECH behält sich vor, diese Richtlinie zur koordinierten Offenlegung von Sicherheitslücken in regelmäßigen Abständen zu aktualisieren, um Änderungen an seinen Produkten, Sicherheitsprozessen, geltenden Standards oder gesetzlichen und behördlichen Anforderungen Rechnung zu tragen.

Die aktuelle Version dieser Richtlinie wird auf der Sicherheitswebsite von LANTECH veröffentlicht.