

1) Zweck

Extrema verpflichtet sich, in seinen Produkten mit digitalen Elementen und den zugehörigen Softwarekomponenten möglicherweise identifizierte Sicherheitslücken verantwortungsvoll und koordiniert zu behandeln. Diese Richtlinie legt fest, wie eine potenzielle Sicherheitslücke an Extrema gemeldet werden kann und welches Verfahren für deren Bewertung, Behandlung und gegebenenfalls Behebung angewendet wird.

2) Wer kann eine Meldung abgeben?

Potenzielle Sicherheitslücken können von jeder natürlichen oder juristischen Person gemeldet werden, die davon Kenntnis erlangt, unabhängig davon, ob sie in einem vertraglichen oder geschäftlichen Verhältnis zu Extrema steht oder nicht.

Als Meldende kommen daher beispielsweise und ohne Anspruch auf Vollständigkeit in Betracht:

- Händler und Vertriebspartner;
- Installateure und Wartungstechniker;
- Nutzer der Produkte;
- IT-Sicherheitsforschende;
- Lieferanten von Komponenten oder Dienstleistungen;
- auf Cybersicherheit spezialisierte Unternehmen;
- Einrichtungen oder Organisationen, die eine potenzielle Sicherheitslücke identifizieren.

3) Wie eine Sicherheitslücke gemeldet werden kann

Meldungen sind an die folgende Kontaktstelle zu richten:

Sicherheitskontakt: security@extrema.it

Die Meldung sollte, soweit verfügbar, Folgendes enthalten:

- Identifizierung des betroffenen Produkts;
- Version des betroffenen Produkts, der Firmware oder der Software;
- Beschreibung der potenziellen Sicherheitslücke;
- die zur Reproduktion des Problems erforderlichen Bedingungen;
- gegebenenfalls technische Nachweise oder für die Überprüfung hilfreiche Informationen;
- mögliche Auswirkungen auf die Sicherheit;
- Kontaktangaben des Meldenden, sofern er kontaktiert werden möchte.

Es ist nicht erforderlich, Informationen bereitzustellen, die der Meldende nicht besitzt oder die er vernünftigerweise nicht beschaffen kann.

4) Schutz des Meldenden

Extrema wird gegen Personen, die Sicherheitslücken nach Treu und Glauben und in Übereinstimmung mit dieser Richtlinie melden, keine rechtlichen Schritte einleiten, sofern die Forschungs- und Meldetätigkeiten nicht zu Verletzungen der Privatsphäre, zur Zerstörung oder Veränderung von Daten oder zu Unterbrechungen oder Beeinträchtigungen der Verfügbarkeit von Diensten führen.

5) Bearbeitung von Meldungen

Extrema wird die eingegangenen Meldungen bewerten und gegebenenfalls eine technische Überprüfung der Sicherheitslücke, eine Risikobewertung sowie die Ermittlung geeigneter Abhilfe- oder Minderungsmaßnahmen durchführen. Sofern angemessen, wird Extrema während des Prozesses der Analyse und Behandlung der Sicherheitslücke mit dem Meldenden im Austausch bleiben.

6) Koordinierte Offenlegung

Extrema wendet ein Verfahren zur koordinierten Offenlegung von Sicherheitslücken (Coordinated Vulnerability Disclosure – CVD) an, das darauf abzielt, die Analyse und Behebung von Sicherheitslücken zu ermöglichen, bevor technische Informationen öffentlich offengelegt werden, die die Ausnutzung der Sicherheitslücke erleichtern könnten. Informationen über eine Sicherheitslücke werden nach dem Need-to-know-Prinzip und unter Berücksichtigung des Risikoniveaus und der Sicherheitsanforderungen mit den betroffenen Parteien geteilt.

7) Informationen für Nutzer

Erfordert eine Sicherheitslücke Maßnahmen durch Nutzer, Installateure oder mit der Wartung beauftragte Personen, wird Extrema, soweit zutreffend, die erforderlichen Informationen und Anweisungen bereitstellen und geeignete Abhilfe- oder Minderungsmaßnahmen verfügbar machen.

8) Meldungen zu Produkten Dritter

Betrifft die Meldung ausschließlich eine Komponente oder ein Produkt eines Dritten, die bzw. das in ein Extrema-Produkt integriert ist, wird Extrema die Meldung selbst bewerten und gegebenenfalls mit dem betreffenden Lieferanten bei der Behandlung der Sicherheitslücke zusammenarbeiten.

9) Kontakt

Für Meldungen von Sicherheitslücken:

E-Mail: security@extrema.it

Für Anfragen zu technischer Unterstützung, Wartung oder Garantie nutzen Sie bitte die üblichen Extrema-Supportkanäle.