Richtlinie zur verantwortungsvollen Offenlegung von Schwachstellen

1. Einleitung und Ziele

Wir nehmen die Sicherheit unserer Produkte und Dienstleistungen sehr ernst und freuen uns über Rückmeldungen von Sicherheitsexperten und Nutzern, um die Sicherheit unserer Produkte und Dienstleistungen zu verbessern.

Diese Richtlinie soll einen klaren Rahmen für das verantwortungsvolle Melden von Schwachstellen schaffen und deren effektive und sichere Behebung gewährleisten.

2. Koordinierte Veröffentlichung

Wir sind bestrebt, die Sicherheit unserer Produkte und Dienstleistungen zu verbessern, und veröffentlichen validierte und relevante Schwachstellen in Form von Security Advisories. Um unsere Kunden zu schützen und eine koordinierte Behebung von Schwachstellen zu gewährleisten, bitten wir darum, entdeckte Schwachstellen vertraulich zu behandeln und nicht zu veröffentlichen, bis Gantner das Problem geprüft hat und geeignete Gegenmaßnahmen umgesetzt oder kommuniziert wurden.

3. Meldekanal

Wenn Sie ein Problem identifiziert haben, dass möglicherweise die Sicherheit unserer Produkte oder Dienstleistungen beeinträchtigen kann, senden Sie bitte eine E-Mail an:

securityalert@gantner.com

4. Schwachstellenmanagement

Wir bemühen uns, den Eingang Ihrer Schwachstellenmeldung innerhalb von 7 Werktagen zu bestätigen und den Triage-Prozess innerhalb von 14 Werktagen abzuschließen. Während des gesamten Prozesses halten wir Sie über den Fortschritt und den Abschluss etwaiger Abhilfemaßnahmen auf dem Laufenden.

Sollten weitere Informationen erforderlich sein, werden wir uns möglicherweise zur Klärung an Sie wenden. Die Behebung gemeldeter Sicherheitslücken wird anhand von Faktoren wie Auswirkung, Schweregrad und Komplexität der Ausnutzung priorisiert. Aufgrund dieser Überlegungen kann es bei einigen Meldungen zu Verzögerungen bei der Triage oder Behebung kommen. Sie können sich gerne nach dem Status erkundigen; wir bitten Sie jedoch, dies nicht öfter als einmal alle 14 Tage zu tun, damit sich unsere Teams auf die Behebungsmaßnahmen konzentrieren können.

5. Grundsätze für Sicherheitsexperten

Wir setzen die Einhaltung von Gesetzen voraus. Das Scannen von Schwachstellen darf nicht als Vorwand für einen Angriff auf ein System oder ein anderes Ziel dienen. Bestimmte Handlungen sind zu unterlassen, zum Beispiel:

> die Verwendung von Social Engineering,
> Kompromittieren des Systems und Aufrechterhalten des Zugriffs auf das System,
> Ändern von Daten, auf die durch Ausnutzung von Sicherheitslücken zugegriffen wird,

- Verwendung von Malware,
- Ausnutzen von Schwachstellen in irgendeiner Weise, die über den Nachweis ihrer Existenz hinausgeht. Um zu beweisen, dass die Schwachstelle existiert, könnte der Meldende nicht-intrusive Methoden verwenden, z.B. das Auflisten eines Systemverzeichnisses,
- Verwendung von Brute-Force, um Zugriff auf Systeme zu erhalten,
- Weitergabe von Sicherheitslücken an Dritte,
- Ausführen von DoS- oder DDoS-Angriffen.

6. Intigriti Bug Bounty and Vulnerability Dislosure Program

Wir ermutigen Ethical Hacker außerdem, Schwachstellen über unser Intigriti Vulnerability Disclosure Program zu melden.

Darüber hinaus laden wir einige unserer Produkte Ethical Hacker ein, über unser SALTO WECOSYSTEM Bug-Bounty-Programms auf Intigriti Schwachstellen zu finden.

Helfen Sie uns, unsere Sicherheit zu stärken – und werden Sie dafür belohnt. Jetzt hier anmelden.