Responsible Disclosure Richtlinie

CRYPTRON Security GmbH

22. Februar 2022

1.1 Responsible Disclosure Richtlinie

In der Computersicherheit ist die koordinierte Offenlegung von Schwachstellen wichtig, daher hat das CRYPTRON Security Research Lab eine Richtlinie dazu geschrieben und wichtige Eckpunkte zusammengefasst.

1.2 Koordinierte Offenlegung von Schwachstellen

Um die besten Praktiken der Branche zu befolgen, basiert unser Prozess der verantwortungsvollen Offenlegung[1] von kritischen Schwachstellen auf der Richtlinie von Google zur Offenlegung von Schwachstellen. https://www.google.com/about/appsecurity

Informationssicherheit und Schwachstellenmanagement sind kein Zustand, sondern ein Prozess.

Sowohl Anbieter als auch Forscher müssen verantwortungsbewusst handeln. Aus diesem Grund hält sich CRYPTRON Security Research Lab an eine 90-Tage-Frist für die Veröffentlichung von Schwachstellen. Wir benachrichtigen Hersteller sofort über Schwachstellen und geben Details erst nach 90 Tagen öffentlich bekannt (oder früher, wenn der Hersteller einen Fix veröffentlicht). Diese Frist kann auf folgende Weise variieren:

- Wenn eine Frist an einem Wochenende oder einem US-Feiertag abläuft, wird die Frist auf den nächsten Werktag verschoben.
- Wenn uns ein Hersteller vor Ablauf der 90-Tage-Frist mitteilt, dass ein Patch an einem bestimmten Tag veröffentlicht werden soll, der innerhalb von 14 Tagen nach der Frist liegt, verschieben wir die öffentliche Bekanntgabe bis zur Verfügbarkeit des Patches.
- Wenn wir eine bisher unbekannte und nicht gepatchte Schwachstelle in einer Software feststellen, die aktiv ausgenutzt wird (ein "0day"), halten wir dringendere Massnahmen - innerhalb von 7 Tagen - für angebracht. Der Grund für diese besondere Bezeichnung ist, dass mit jedem Tag, an dem eine aktiv ausgenutzte Sicherheitslücke der Öffentlichkeit nicht bekannt gegeben wird und nicht gepatcht ist, mehr Geräte oder Konten gefährdet werden. Sieben Tage sind ein aggressiver Zeitplan und könnten für einige Anbieter zu kurz sein, um ihre Produkte zu aktualisieren, aber es sollte genug Zeit sein, um Hinweise auf mögliche Abhilfemaßnahmen zu veröffentlichen, wie z. B. die vorübergehende Deaktivierung eines Dienstes, die Einschränkung des Zugriffs oder die Kontaktaufnahme mit dem Anbieter für weitere Informationen. Wenn 7 Tage ohne Patch oder Hinweis verstrichen sind, werden wir die Forscher dabei unterstützen, Details zur Verfügung zu stellen, damit die Benutzer selbst Massnahmen zum Schutz ergreifen können.

[1] https://en.wikipedia.org/wiki/Coordinated_vulnerability_disclosure

- Wenn Geräte oder Software, die dem Offenlegungsprozess unterliegen, vom Hersteller ausdrücklich als End-of-Life oder End-of-Support bezeichnet werden, begrenzen wir die Frist auf 30 Tage, es sei denn, wir erhalten eine positive Bestätigung, dass ein Out-of-Band-Patch vom Hersteller herausgegeben wird.
- Wie immer behalten wir uns das Recht vor, die Fristen aufgrund extremer Umstände vorzuverlegen oder zu verkürzen. Wir verpflichten uns weiterhin, alle Anbieter gleich zu behandeln.

Wir können uns während des Prozesses der verantwortungsvollen Offenlegung mit den internationalen Computer Emergency Response Teams (CERTs[2]) oder dem Nationalen Zentrum für Cybersicherheit (NCSC[3]) in Verbindung setzen, um die Veröffentlichung zu koordinieren, falls kritische Sicherheitslücken festgestellt wurden, die eine grosse Benutzerbasis oder kritische ICT Systeme betreffen.

1.3 Zusammenarbeit mit Software-, oder Hardware Hertellern

CRYPTRON Security Research Lab verpflichtet sich, angemessene Anstrengungen zu unternehmen, um die Kommunikation mit dem betroffenen Hersteller herzustellen. Wir versuchen, den öffentlich zugänglichen Sicherheitskontakt zu nutzen, andernfalls kontaktieren wir den Herstellersupport über öffentlich zugängliche Mechanismen und/oder senden E-Mails an security@, support@, info@ Adressen.
Wir bitten die Anbieter, einen geeigneten Sicherheitskontakt einschließlich Verschlüsselungszertifikaten zur Verfügung zu stellen, um die Vertraulichkeit des Sicherheitshinweises oder jeder weiteren Kommunikation zu schützen.

In keinem Fall wird eine Sicherheitslücke "verschwiegen", weil ein Produktanbieter sie nicht beheben möchte. Um den Prozess transparent zu halten, fügen wir die Zusammenfassung der Kommunikation mit dem Hersteller in den Hinweis ein.
Wir ermutigen die Hersteller, uns aktualisierte Informationen zur Verfügung zu stellen, die in den endgültigen Sicherheitshinweis aufgenommen werden. Dazu könnten gehören: die von dem Fehler betroffenen Softwareversionen oder Hardwareversionen, die Nummer der behobenen Version und eine Möglichkeit, das Update zu erhalten (z. B. die URL einer Website, von der das Sicherheitsupdate oder die neue Version heruntergeladen werden kann). Wir empfehlen dem Anbieter, die CVE-Nummern für die entsprechenden Sicherheitslücken anzufordern.
Wir begrüßen es, wenn die Hersteller in den Versionshinweisen und Ankündigungen den/die Forscher, die das Sicherheitsproblem identifiziert haben, und das CRYPTRON Security Research Lab nennen.

1.4 CRYPTRON Security Research Labs

Das CRYPTRON Security Research Lab ist die integrierte Forschungseinrichtung der CRYPTRON Security GmbH mit Sitz in der Schweiz. Für Anfragen, Feedback oder Kommentare wenden Sie sich bitte an info@cryptron.ch.

Securitytxt.org (RFC 8615) definiert einen Standard, der Organisationen dabei hilft, den Prozess für Sicherheitsforscher zur sicheren Offenlegung von Sicherheitslücken zu definieren. Security.txt-Dateien wurden bereits von Google, Facebook, GitHub, der britischen Regierung und vielen anderen Organisationen eingeführt. Das CRYPTRON Security Research Lab verwendet ebenfalls eine security.txt Datei unter folgendem Link https://www.cryptron.ch/files/Cryptron/.well-known/security.txt.

[2] https://en.wikipedia.org/wiki/Computer_emergency_response_team#National_or_economic_region_teams
[3] https://www.ncsc.admin.ch/ncsc/en/home.html