Einführung

«Responsible Disclosure» ist ein Verfahren, das es IT-Sicherheitsforschern ermöglicht, gefundene Schwachstellen sicher an die zuständigen Stellen innerhalb der Organisation zu melden. Dieses Dokument beschreibt den Inhalt der Policy.

Die *ETH Zürich* ist bestrebt, die bewährten IT-Sicherheitspraktiken zum Schutz von Daten und Systemen umzusetzen. Diese Policy soll Sicherheitsforschern Richtlinien für die Entdeckung von Schwachstellen vermitteln und unsere Präferenzen für die Übermittlung entdeckter Schwachstellen an uns aufzeigen. Weiter beschreiben wir, welche Systeme und Arten von Forschung unter diese Richtlinie fallen.

Grundsätze

Im Rahmen dieser Policy bezeichnet der Begriff "Forschung" Aktivitäten, bei denen Sie:

- uns so schnell wie möglich benachrichtigen, nachdem Sie ein erhebliches reales oder potenzielles IT-Sicherheitsproblem entdeckt haben.
- alle Anstrengungen unternehmen, um Verletzungen der Privatsphäre, Beeinträchtigungen der Benutzerfreundlichkeit, Störungen der Produktionssysteme und die Zerstörung oder Manipulation von Daten zu vermeiden.
- nutzen Sie Exploits nur in dem Umfang, der notwendig ist, um das Vorhandensein einer Sicherheitslücke zu bestätigen. Verwenden Sie einen Exploit nicht, um Daten zu kompromittieren oder zu exfiltrieren, dauerhaften Befehlszeilenzugriff zu erlangen oder den Exploit zu nutzen, um auf andere Systeme überzugehen.
- Geben Sie uns eine angemessene Zeitspanne, um das Problem zu lösen, bevor Sie es öffentlich machen.
- reichen Sie keine Meldungen von minderer Qualität ein.

Wenn eine Sicherheitslücke, die ein System der ETH Zürich betrifft, in Übereinstimmung mit den festgelegten Regeln gemeldet wird und der Meldende in gutem Glauben und ohne betrügerische Absicht oder die Absicht, Schaden anzurichten, handelt, wird die ETH Zürich keine zivil- oder strafrechtlichen Schritte gegen Sie einleiten.

Testmethoden

Die folgenden Testmethoden sind ausdrücklich untersagt:

- Netzwerk-Denial-of-Service-Tests (DoS oder DDoS) oder andere Tests, die den Zugriff auf ein System oder Daten beeinträchtigen oder beschädigen.
- Physische Tests (z. B. Bürozugang, offene Türen, Auflauern), Social Engineering (z. B. Phishing, Vishing) oder andere nichttechnische Schwachstellentests.

Sobald Sie eine Schwachstelle festgestellt haben oder auf sensible Daten gestossen sind (einschliesslich personenbezogener Daten, finanzieller Informationen oder geschützter Informationen oder Geschäftsgeheimnisse einer Partei), müssen Sie Ihren Test beenden, uns sofort benachrichtigen und diese Daten nicht an Dritte weitergeben.

Scope

Diese Richtlinie gilt für die folgenden Systeme und Dienste der zugehörigen Domains:

- ethz.ch (einschliesslich aller On-Premises-Hosts mit privaten IPs (z.B. RFC1918)
- Gemäss WHOIS
    - die Organisation (Feld "org"), die dem Eintrag ORG-ETHZ1-RIPE entspricht.
    - die Rollen admin-c oder tech-c, die "HE688-RIPE" (Hostmaster ETHZ) definieren.

Alle Dienste oder Systeme der Domäne(n), die oben nicht aufgeführt sind, sind vom Scope ausgeschlossen und nicht für die Prüfung zugelassen. Schwachstellen, die in Systemen anderer Institutionen des ETH-Bereichs (z.B. Empa, Eawag, etc.) gefunden werden, fallen nicht in den Geltungsbereich dieser Richtlinie und sollten gemäss deren Disclosure Policy (falls vorhanden) direkt an den Anhang gemeldet werden. Wenn Sie nicht sicher sind, ob ein System in den Geltungsbereich fällt oder nicht, wenden Sie sich an das zuständige Sicherheitsteam für den Domain-Namen des Systems, der in einem WHOIS-Register aufgeführt ist (z.B. https://www.ripe.net).

Kontakt und Einreichung

Füllen Sie das untenstehende Formular aus und geben Sie Details zu Ihrer Entdeckung an. Falls vorhanden, fügen Sie bitte Ihren öffentlichen PGP-Schlüssel bei, damit die ETH Zürich die Einsendungen validieren kann.

Reichen Sie Ihre Schwachstellenfunde nur an **security@ethz.ch** ein.

Für die verschlüsselte Kommunikation verwenden Sie bitte den PGP-Schlüssel von **security@ethz.ch**

- Key-ID: 0x6EEEFBFFD6437004
- Fingerprint: 2CC2 9A19 4B25 DDD0 B750 B48B 6EEE FBFF D643 7004

Geben Sie so viele Informationen wie möglich an, damit die Schwachstelle reproduziert werden kann. Dies hilft, den Prozess zu beschleunigen. Bei komplexeren Schwachstellen muss die ETH Zürich unter Umständen direkt mit Ihnen kommunizieren. Bitte geben Sie mindestens eine E-Mail-Adresse oder Telefonnummer an.

Was wir uns von Ihnen wünschen

Um uns bei der Einordnung und Priorisierung der Meldungen zu helfen, empfehlen wir, dass Ihre Meldungen:

- Beschreiben Sie den Ort, an dem die Schwachstelle entdeckt wurde, und die möglichen Auswirkungen einer Ausnutzung. Einsendungen, die diese Informationen nicht enthalten, werden ignoriert.
- eine detaillierte Beschreibung der Schritte, die zur Reproduktion der Schwachstelle erforderlich sind (Proof-of-Concept-Skripte oder Bildschirmfotos sind hilfreich).
- Geben Sie relevante Referenzen für die Schwachstelle an: z. B. CVE, Sicherheitsbulletins usw.

Sie können Ihre Schwachstellenberichte auch anonym an die ETH Zürich senden. Die Beiträge sollten möglichst auf Englisch oder Deutsch verfasst sein.

Was Sie von uns erwarten können

Wenn Sie sich entscheiden, uns Ihre Kontaktdaten mitzuteilen, werden wir uns so offen und so schnell wie möglich mit Ihnen darüber austauschen. Die ETH Zürich wird

- von Fall zu Fall entscheiden, ob eine Reaktion notwendig und gerechtfertigt ist.
- behandeln Meldungen vertraulich und geben die persönlichen Daten der meldenden oder empfangenden Organisation nicht ohne deren Zustimmung weiter.
- je nach den betroffenen Stellen und der Art der festgestellten Schwachstelle die zuständigen Stellen auf die Schwachstelle aufmerksam machen. Der Besitzer des betroffenen IT-Systems bleibt für das System und mögliche Behebungsmassnahmen verantwortlich.

Bestätigung und Belohnungen

Die ETH Zürich ist nicht in der Lage, Meldungen durch die Veröffentlichung von Ergebnissen (z.B. Akkreditierung oder Auflistung in der Hall of Fame) oder durch die Zahlung von Bug Bounty Prämien zu belohnen. Wir hoffen, dass die Forschenden ihre Ergebnisse in gutem Glauben und im Interesse der Förderung der IT-Sicherheit auf globaler Ebene einreichen werden.

Formular zur Meldung von Schwachstellen

Melden Sie Ihren Ergebnissen an: ***security@ethz.ch***

Teilen Sie mit, wo Sie die Schwachstelle gefunden haben.
Beispiele sind Hostname, URL, IP-Adresse oder Service.

Beschreiben Sie die Schwachstelle und ihre möglichen Auswirkungen.

Beschreiben Sie detailliert die notwendigen Schritte, um die Schwachstelle zu reproduzieren.
*Links zu Proof-of-Concept-Skripten oder Screenshots sind hilfreich**

Gibt es noch etwas, das wir wissen sollten?

Sie können uns Ihre Kontaktdaten mitteilen, damit wir uns bei Bedarf mit Ihnen in Verbindung setzen können.
E-Mail-Adresse, Telefonnummer, andere Websites

Fügen Sie Ihre PGP-Signatur hinzu, um Ihre Identität zu belegen.

* Beachten Sie, dass Anhänge wie Skripte, Programme, Screenshots usw. von Virenscanprogrammen herausgefiltert werden oder dazu führen können, dass die gesamte E-Mail vollständig blockiert wird. Bitte achten Sie auf den Inhalt der gesendeten Informationen.