PRODUCT VULNERABILITY DISCLOSURE POLICY

Plantronics + Polycom = Poly

Information security is a top priority for Poly and we are committed to providing high levels of security and assurance in all our products and services. New security threats and vulnerabilities are discovered around the world by security researchers, ethical hackers, customers, academics, and the community, almost daily. With the collective goal of helping to keep systems and data secure, we are committed to addressing security issues through a coordinated and constructive approach to improve our products and services, and to better protect our customers.

To support the discovery and reporting of vulnerabilities and increase the security posture of our products, we welcome and encourage members of the security research community who find vulnerabilities, bring them to our attention, and work with us in a coordinated effort so that security fixes can be issued to all impacted customers.

Products and Services in Scope

This policy addresses all products, software and hardware, sold under the Plantronics, Polycom and Poly brand names made available to the general public or enrolled in an officially sanctioned pre-release or beta program. If contractual obligations exist between Poly and a partner where the partner must address an identified vulnerability, the terms of the agreement between the partner and Poly shall prevail over the terms set forth in this policy.

Out of Scope

Misconfiguration of devices not aligned with best practices;

Vulnerabilities affecting outdated software or products that are no longer supported;

Attacks that require the use of phishing or other types of social engineering;

Acquisitions as integration efforts may not be complete; and

Non-Poly sites, cloud service providers, sites belonging to other individuals, organizations and customers.

Guidelines

Do not exploit any vulnerability beyond the scope of testing required to prove that a vulnerability exists;

Do not store, copy, use, retain, transfer or otherwise access sensitive or personally identifiable data;

Do not access, delete or modify our data or our customer's data or intentionally compromise the privacy or safety of Poly customers or any third parties;

Do not interrupt or degrade our services (including denial of service) as this may adversely impact normal operations;

Avoid privacy violations and contact us immediately if you do inadvertently encounter customer data;

Please contact us for clarification before engaging in conduct that may be inconsistent with or unaddressed by this policy; and

Comply with all applicable laws.

Legal Action

If you follow these guidelines and adhere to this policy, we will not pursue civil action or support any legal action related to your research for accidental, good faith violations of its policy, or initiate a complaint to law enforcement for unintentional violations. We consider research activities conducted in a manner consistent with this policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act.

Reporting Vulnerabilities

If you believe you have discovered a vulnerability in a Poly product or service, please submit a vulnerability report to Poly's Product Security Incident Response Team (PSIRT) by sending an email to security@polycom.com

To ensure confidentiality when sending sensitive information to Poly via email, we encourage you to encrypt your messages.

Please include a detailed description of the vulnerability, including: the type of issue; product, version, and configuration of software containing the issue; and where possible, step-by-step instructions on how to reproduce the vulnerability along with screenshots. Demonstrating the existence of the vulnerability will help us validate the vulnerability.

In the event that sensitive or personally identifiable data is disclosed, comply with all applicable laws and do not save, store, transfer or otherwise access that data.

Upon receipt of your report, we will provide a timely acknowledgment to your report. We will assign resources to investigate the issue to verify the existence of the vulnerability using the information provided and provide notification that we have confirmed the vulnerability. Given the complexity of some environments and configurations, we may request additional information if we are unable to verify vulnerability.

Poly's Product Security Incident Response Team may consult with legal counsel before responding to unanticipated questions or reports.

We will provide an update when the vulnerability analysis has been completed. We will then provide you with an expected timeline for patches and fixes. We will address the vulnerability and release an update or patch to the software. We make the best effort possible to resolve vulnerabilities in supported products as quickly as possible. Delivery of patches or fixes will be prioritized by criticality, product impacted, and fix complexity, and quality testing. Due these factors and unforeseen extenuating circumstances, we unable guarantee a level of response.

Public Notification and Acknowledgement

If applicable, Poly will coordinate public notification of a validated vulnerability with you. When possible, we would prefer that our respective public disclosures be posted simultaneously.

In order to protect our customers and give them adequate time to update any vulnerable systems, Poly requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, informed customers if needed and released a fix addressing the vulnerability.

Poly will acknowledge and credit, with their permission, in Poly's security advisory of an identified vulnerability, third party researchers who follow a responsible, coordinated vulnerability disclosure practice as outlined in this policy, whereby the vulnerability is not disclosed prematurely or before Poly has made a patch available for its customers. Third party reporters also have the option to remain anonymous if they so desire.

Poly does not credit its own employees, their family members, contractors or agents for identifying any vulnerabilities in Poly's security advisories.

Security advisories related to our products and services are posted on our security web site at: https://support.polycom.com/content/support/security-center.html

Compensation Requests

Submissions made under duress or requests for monetary compensation in connection with any identified or suspected vulnerability will be deemed non-compliant with this Vulnerability Disclosure Policy.

Citation and Credit for DoJ Framework: https://www.justice.gov/criminal-ccips/page/file/983996/download