DISCLOSURE POLICY

Team82 Coordinated Disclosure Policy

Challenges

As Team82 is very active in security research, the purpose of this Coordinated Disclosure policy is to (1) ensure that Team82 operates in accordance with an established and clear set of standards and practices, and (2) provides transparency with the cybersecurity community regarding Team82's practices.

Mission

Team82 is committed to privately reporting vulnerabilities to affected vendors in a coordinated, timely manner in order to ensure the security and safety of the cyber-physical systems ecosystem worldwide. We understand the community is a vital part of this process, and we want to explain our coordinated disclosure efforts. Team82 will adhere to the following reporting and disclosure process when its researchers discover vulnerabilities in products and services.

Procedures

The following are the procedures that Team82 researchers will follow whenever a third party vulnerability is discovered.:

- Once a vulnerability has been identified and analyzed, Team82 will attempt to establish confidential communication with the affected vendor.
- Team82's initial outreach will include an attempt to exchange PGP keys in order to securely exchange vulnerability information.
- Team82 will then provide a detailed technical description about the security issue to the vendor.
- The vendor will have 15 days to acknowledge receipt and respond.
- There will be instances when Team82 will also inform CISA, CERT VDE, or similar reporting agency in parallel to notifying an affected vendor.

Disclosure. Initial vendor outreach also includes a statement regarding Team82's policy that such vulnerability reports would be subject to an industry-standard 90-day public disclosure deadline:

"This vulnerability is subject to a 90-day disclosure deadline; after 90 days, if a patch or mitigation has not been made available, Team82 will share information about this vulnerability with the public."

- Should the vendor fail to answer within 15 days, Team82 will notify CISA, CERT VDE, or similar reporting agency and provide them with a description of the vulnerability(ies).

- Once patches are made available by the affected vendor to users, or if the 90-day disclosure deadline passes, Team82 will publish a public report informing users, and will provide additional details once a patch is released or advisory issued by the affected vendor(s).
- Team82 is amenable to working closely with vendors on reasonable deadline extensions should the 90-day deadline not be feasible for patches or mitigations to be made available.

Past the 90-Day Deadline

If a vendor is unresponsive and misses the 90-day deadline:

- Again, Team82 is amenable to working closely with vendors on reasonable deadline extensions should the 90-day deadline not be feasible for patches or mitigations to be made available.
- Team82 will communicate its intention to publicly acknowledge it has found vulnerabilities in the affected vendor's product, and will provide additional details once a patch is released or advisory issued by the affected vendor(s).
- Team82 will be discriminating about what it discloses in these instances, i.e., only part of the relevant exploit chain, or only high-level details that would force an attacker to expend significant resources in order to carry out the research and exploit the flaw in question.
- Team82's approach is meant to incentivize affected vendors to provide its users with timely patches and/or mitigation.
- Regardless of vulnerability severity or scale of distribution of the affected product, Team82 will not publish full technical details about zero days.
- Team82 will publish a blog explaining that it has found vulnerabilities in an affected product and provide limited details about the flaws. Social media posts will also be made.asset management, and streamlined operational workflows for maintenance and security across mission- critical environments.

Timeline

Discovery

- Attempt to securely communicate with vendor
- Signatures developed for Team82 customers

15 Days

- Second secure email sent to vendor
- CISA, CERT VDE, or similar reporting agency notification

60 Days

- Final reminder email sent to the vendor, informing them of the tentative release date of Team82's public disclosure

90 Days

- Public disclosure: Publication of Team82 research paper/blog/social media outreach

Past the 90-Day Deadline

Email: secure@claroty.com

PGP key: https://claroty.com/team82/pgp-key

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.