CLAROTY

CLAROTY COORDINATED DISCLOSURE POLICY

Challenges

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

Mission

Claroty is committed to privately reporting vulnerabilities to affected vendors in a coordinated, timely manner in order to ensure the security and safety of the OT ecosystem worldwide. We understand the community is a vital part of this process, and we want to explain our coordinated disclosure efforts. Claroty 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 Claroty researchers will follow whenever a third party vulnerability is discovered.

- Once a vulnerability has been identified and analyzed, Claroty will attempt to establish confidential communication with the affected vendor.
- Claroty's initial outreach will include an attempt to exchange PGP keys in order to securely exchange vulnerability information.
- Claroty 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 Claroty will also inform a CERT in parallel to notifying an affected vendor.

Disclosure. Initial vendor outreach also includes a statement regarding Claroty'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, Claroty will share information about this vulnerability with the public."

- Should the vendor fail to answer within 15 days, Claroty will notify the relevant CERT, such as the Industrial Control System Computer Emergency Response Team (ICS-CERT) 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, Claroty 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).
- Claroty 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, Claroty 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.
- Claroty 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).
- Claroty 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.
- Claroty'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, Claroty will not publish full technical details about zero days.
- Claroty 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.

Timeline

Discovery

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

15 Days

- Second secure email sent to vendor
- CERT/ICS-CERT notification

60 Days

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

90 Days

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

Claroty Contact Information

Email: secure@claroty.com

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

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.

For more information, visit www.claroty.com.