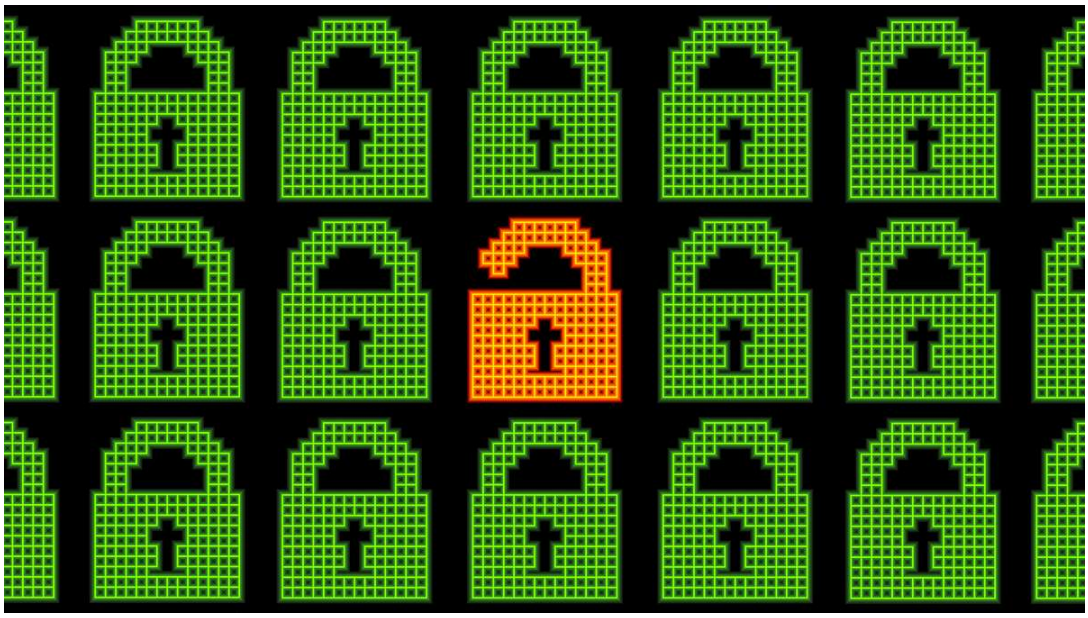
The Daily Swig
Cybersecurity news and views

FIRST updates guidelines for multi-party vulnerability disclosure

Jessica Haworth 18 May 2020 at 11:46 UTC
Updated: 19 May 2020 at 07:50 UTC

Vulnerabilities | Industry News | Bug Bounty

Best practice playbook expanded to include clear comms, safe harbor clauses, and disclosure embargoes



The Forum of Incident Response and Security Teams (FIRST) has released updated guidelines to assist and simplify multi-party, coordinated vulnerability disclosure.

FIRST is an international confederation of incident response teams that tasks itself with promoting security best practices and maintaining the widely-used CVSS scoring system.

Previous vulnerability disclosure guidelines released by the non-profit have been mainly focused on relationships between two parties: the stakeholder (vendor or organization) and the bug finder.

However, as software development becomes more complex and connected to supply chains, coordinated vulnerability disclosure practices need to evolve, explained Art Manion, vulnerability analysis technical manager at CERT Coordination Center.

Multi-party vulnerability disclosure

A new set of guidelines has been produced by FIRST, in collaboration with the National Telecommunications and Information Administration (NTIA).

The document is aimed at anyone involved in multi-party vulnerability disclosures – from security researchers to incident response teams.

The updated advice (version 1.1) was unveiled earlier this month to address shortcomings in how multiple parties should engage and cooperate during the security vulnerability disclosure process.

"Factors such as a vibrant open source development community, the proliferation of bug bounty programs, [and] increasing supply chain complexity… are just a few of the complications," the report reads.

"Examples such as Heartbleed highlight these coordination and disclosure challenges."

The Heartbleed bug, a serious flaw in OpenSSL, was first disclosed in 2014. At the time of exposure, around 17% – approximately 500,000 – of certified secure web servers were thought to be vulnerable.

"This document is a collection of best current practices that consider more complex and typical real-life scenarios that extend past a single researcher reporting a vulnerability to a single company," the report adds.

Best practices

The document includes strong suggestions on how to implement best practices, policy, and processes for coordinated vulnerability disclosure.

Latest Posts

Exploit drops for RCE bug ir Control Web Panel
Vendor patched the vulnerability in after a red team alert

CORS for concern
Tesla tackles misconfigurations tha internal networks vulnerable

Devs urged to rotate secrets CircleCI suffers breach
DevOps platform advises custome revoke API tokens

It differs from ISO standards that are usually written for one group – vendors – focusing on bilateral disclosure.

Instead, it provides "practical guidance" for all possible stakeholders within the supply chain.

RECOMMENDED FIRST calls for enhanced collaboration among incident response teams

Serge Droz, FIRST chair, told *The Daily Swig*: "There is effectively no deviation. The FIRST document gives more actionable guidance and detail than the ISO standard, and both documents are in harmony with each other.

"Version 1 of the document briefly introduced the roles and responsibilities of all parties involved in the discourse process and then discussed examples.

"The updated version adds more conceptional information and spells out the best current practices. In essence it implements the lessons learned since the inception of the first version.

"Ultimately these guidelines should help people in the field to react better," added Droz.

Timelines and thresholds

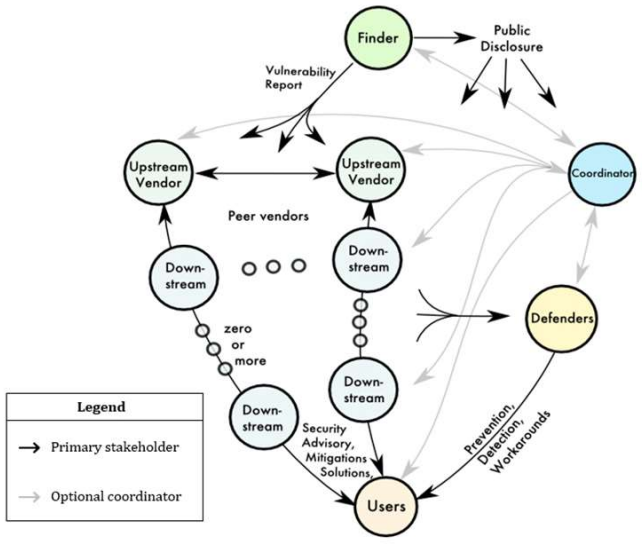
Recommendations include establishing strong relationships between stakeholders and researchers, by publishing "actionable public vulnerability coordination and disclosure policies and expectations, including timelines and thresholds for disclosure".

While a large proportion of the security community adheres to a 90-day disclosure timeline, perhaps most notably observed by Google's Project Zero, FIRST does not recommend a set timeline for remediation, instead encouraging an embargo period.

Other suggestions include maintaining clear and consistent communications between a vendor, vulnerability finder, and other parties both prior to and after discovery.

"Vendors should provide currently accepted contact mechanisms, such as security@ email addresses and 'slash security' (/security) web pages," the document reads.

It continues: "All parties should provide information to help other stakeholders assess severity, priority, and risk associated with vulnerabilities. The CVSS is one such option."



Stakeholder roles and communication paths (Image credit: First.org)

Maintaining trust

Stakeholders should build and maintain trust, for example by launching bug bounty programs or promising safe harbor, and should avoid escalation to any extent – including legal action.

They should also respond quickly to security disclosures, and should appoint a co-ordinator, if appropriate, to "provide additional technical, impact, and scope analysis to researchers, vendors, and other stakeholders, particularly when there is disagreement".

Multiple co-ordinators can be appointed if needed, though one should be named "lead co-ordinator" to minimize confusion.

The document also includes use cases that set out how to appropriately deal with a multi-party security disclosure, from best to worst case scenarios.

So far, Droz notes, the feedback has been extremely positive from vendors who deal with such issues on a regular basis.

He added: "I am proud that FIRST was able to bring these stakeholders together to work on this very important document."

READ MORE Security.txt – IESG issues final call for comment on proposed vulnerability reporting standard

Vulnerabilities | Industry News | Bug Bounty | IoT | Secure Development | Hacking News | Organizations | US | Open Source Software

Jessica Haworth

@JesscaHaworth

Related stories

Exploit drops for RCE bug in Control Web Panel

06 January 2023

CORS for concern

Tesla tackles misconfigurations that left internal networks vulnerable

05 January 2023

Devs urged to rotate secrets after CircleCI suffers breach

05 January 2023

Car companies massively expose to web vulnerabili

04 January 2023