Vulnerability Disclosure Policy

Overview

CodeSentry is committed to improving the security of software ecosystems through responsible vulnerability research and disclosure. This policy outlines our approach to disclosing vulnerabilities we discover in third-party software and systems.

Disclosure Timeline

1. When CodeSentry discovers a vulnerability, we promptly report it to the affected vendor.
2. The affected vendor has 90 days from the initial report to release a patch or mitigation.
3. After 90 days, or when a patch becomes available (whichever is earlier), CodeSentry will publicly disclose the vulnerability.
4. In exceptional circumstances, this deadline may be extended or shortened as detailed below.

Extensions

- If a vendor is actively working on a fix but requires additional time, they can request a 14-day extension.
- Extensions are granted at CodeSentry's discretion and are typically limited to one per vulnerability.
- Vendors must provide a compelling reason and demonstrate significant progress towards a fix.

Early Disclosure

CodeSentry may choose to disclose a vulnerability earlier than 90 days if:

1. The vulnerability is being actively exploited in the wild.

2. The vendor releases a patch before the 90-day deadline.
3. The vendor publishes information about the vulnerability before the deadline.

Grace Periods

- If the 90-day deadline would expire on a weekend or US public holiday, it will be moved to the next normal workday.
- A 14-day grace period may be applied if a vendor notifies us that a patch is scheduled for release within this additional time.

Incomplete Fixes

If a vendor releases an incomplete or incorrect fix, CodeSentry will:

1. Notify the vendor immediately.
2. Work with the vendor to improve the fix.
3. If necessary, treat this as a new vulnerability with a new 90-day disclosure timeline.

Public Disclosure Process

When disclosing a vulnerability, CodeSentry will:

1. Publish a detailed technical write-up on our blog.
2. Release any proof-of-concept code or tools used to identify the vulnerability.
3. Assign a unique identifier to the vulnerability for tracking purposes.
4. Host the vulnerability details on CodeSentry's Demo Dashboard.

Coordination with Other Parties

CodeSentry will work to coordinate disclosure with:

- The affected vendor(s)
- Other security researchers who may have independently discovered the same issue
- National CERT teams, when appropriate

Policy Updates

This policy may be updated periodically. The most current version will always be available on our website.

Website: https://codesentry.sh/vulnerability-disclosure-policy/

Contact

To report vulnerabilities to CodeSentry or to contact us regarding this policy, please email: hello@codesentry.org

Last Updated: June 19, 2024