
Disclosure

No Disclosure

When a vulnerability is found, all information about the vulnerability is kept private. Sometimes this is enforced by non-disclosure agreements (NDAs). Vendors sometimes prefer this scenario to protect secrets, as well as certain researchers that wish to do the same.

Limited Disclosure

When a vulnerability is found, only some information about the vulnerability is disclosed. The goal is typically to slow down reverse engineering and exploit development long enough for a fix to be developed and deployed. This is done by withholding proof of concept code or other technical details of the vulnerability.

Full Disclosure

When a vulnerability is found by a reporter, all information about the vulnerability including proof of concept should be disclosed immediately. The belief is that this disclosure serves the greater good by allowing consumers to be aware of issues in their products, and demand action from vendors, as well as have information available to make more informed purchasing decisions. Security researchers tend to favor this approach. The vendor is typically not informed prior to disclosure, or at least has a very small window (typically < 1 day) to act. Alternately, this type of disclosure may also be performed by the vendor themselves: many open source projects, for example, handle security issues in the open in order to maximize review of the vulnerability and testing of the proposed solution.

Coordinated Disclosure

Coordinated Disclosure is the CERT/CC's preferred terminology for the older "Responsible Disclosure". Among others, Microsoft has advocated for coordinated disclosure. Otherwise, Coordinated Disclosure and Responsible Disclosure are the same thing. Often, you will see Coordinated Vulnerability Disclosure abbreviated as CVD.

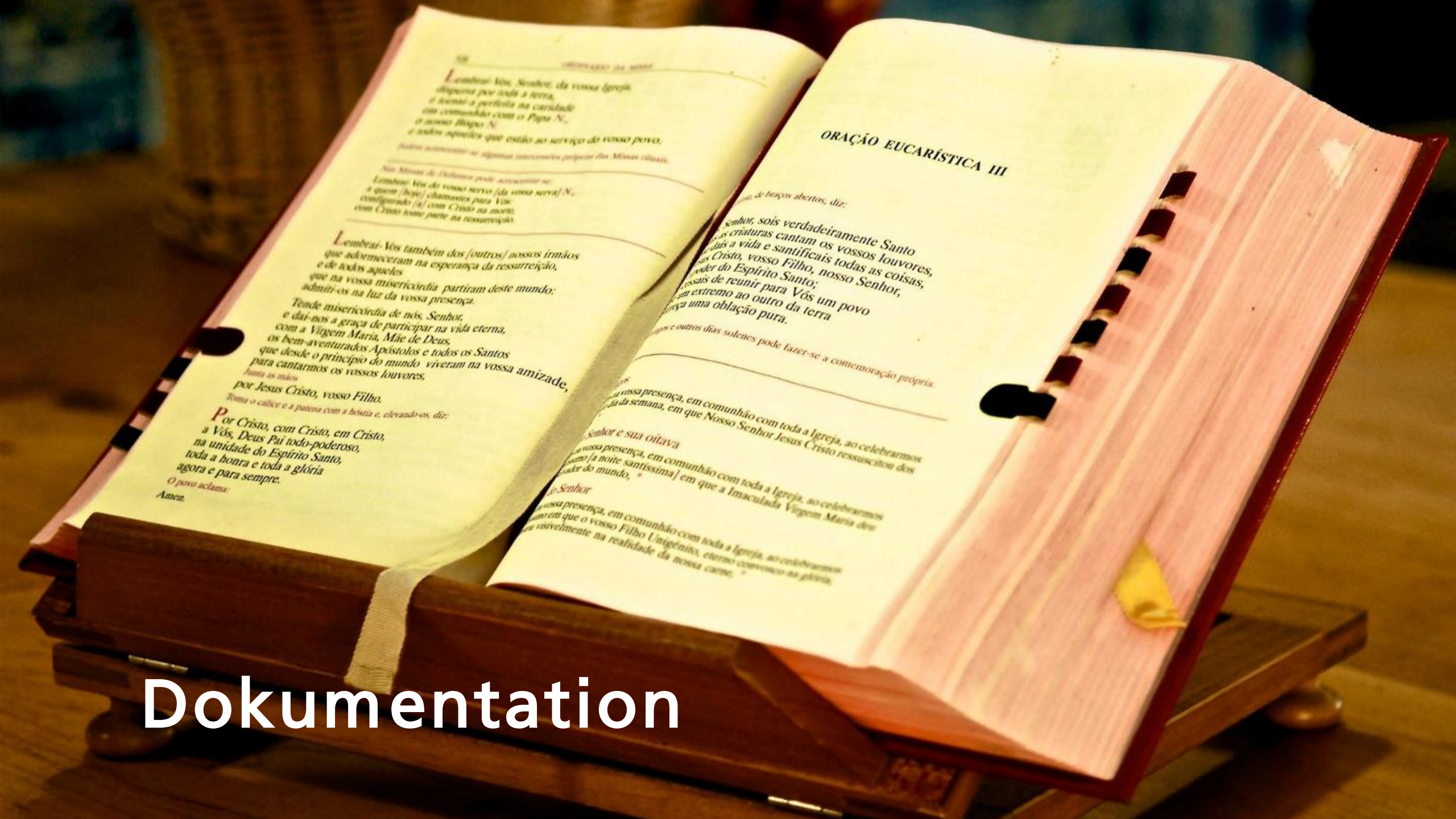
Responsible Disclosure

When a vulnerability is found by a reporter, the reporter informs the vendor and suggests a timeline for disclosure. The amount of time varies greatly based on the organization. The vendor and reporter typically work together to provide a simultaneous public disclosure after a patch is ready. The disclosure may be Limited Disclosure or Full Disclosure after the timeline has expired. In cases where the vendor and reporter do not agree on a timeline, or the vendor is unresponsive, the reporter may publish anyway at the end of the original proposed timeline. In the CERT/CC's opinion, the term "responsible" is too vague. The word "responsible" tends to draw focus toward "good" and "bad", rather than objectively searching for a way to address a problem that was discovered.

Responsible Disclosure

Responsible Disclosure

- Bug finden
- Bug Dokumentieren
- Hersteller kontaktieren
  - PGP Key oder S/MIME Zertifikat bekommen
  - Dann doch verschlüsseltes zip verwenden
- Hersteller Bug erklären
- Hersteller sagen wie er es fixen soll und warum
- Nach 90 Tagen veröffentlichen



Dokumentation

Dokumentation

- Titel
- Betrifft
- Erfordert
- Ermöglicht
- Beschreibung
- Ergebnis
- Auswirkung
- Empfehlung
- Kommentar
- AN: bughunting@sit.fraunhofer.de

Schwäche: Administrator kann ein Nutzerpasswort zu einem leeren Passwort ändern

Betrifft

Funktionalität zum Ändern des Nutzerpassworts.

Erfordert

Einen Account mit Administratorrechten.

Ermöglicht

(Versehentliches) Setzen eines leeren Passworts für einen Nutzer.

Beschreibung

Es wird getestet, ob eine Passwort Policy beim Ändern des Nutzerpasswortes durch den Administrator vorhanden ist.

Ergebnis

Beim Ändern des Nutzerpasswortes wird keine Passwort Policy vorgegeben. In der Benutzerverwaltung kann der Administrator auf das Schlüsselicon klicken, um das Passwort eines Nutzers zu ändern. Wenn dann ohne Eingabe eines Passwortes auf "Änderungen speichern" geklickt wird, kann sich der Nutzer ganz ohne Passwort einloggen.

Auswirkungen

Ohne jegliches Durchsetzen der einer Passwort Policy können Administratoren dazu verleitet werden, sehr schwache Passwörter zu vergeben. In diesem Fall kann auch kein Passwort gesetzt werden, was dazu führen kann, dass ein Administrator versehentlich das Passwort eines Nutzers auf das leere Passwort ändert. Bei einem leeren Passwort, kann sich jeder mit dem Benutzernamen einloggen, da kein Passwort erforderlich ist.

Empfehlung

Eine Passwort Policy sollte durchgesetzt werden. Leere Passwörter dürfen nicht akzeptiert werden.

Kommentar

Edited 2 weeks ago by Philipp Roskosch


START