

Security Incident Severity Matrix

Security Incident Severity Matrix

Adapted from GitLab's Security Incident Severity Matrix.

Purpose

A standard way to classify how serious a security incident is. Severity decides how fast we respond, who gets involved and who we tell. It is set during the first triage.

Matrix

Severity	Impact	NFE response	Examples
S1 Critical	Customers lose power or their data is exposed, or severe damage to NFE (money, reputation, funder trust)	Drop everything. All available team members help. Updates at least every few hours.	Confirmed breach of customer or financial data. An attacker controls an admin account (Nextcloud <code>admins</code> , server root, ERPNext admin). Remote control of meters or inverters at a site. Ransomware on a shared system.
S2 High	Significant disruption for customers or the team, or likely damage to NFE	Named responder; same-day action; daily updates	A mailbox used to send spam (Mar–Apr 2026, Aug–Sep 2026). Suspected unauthorised access to Nextcloud or mail. Malware on a team laptop. Our mail relay IP listed on Spamhaus.
S3 Medium	Moderate impact; work is hampered	Handle within the week alongside normal work	A phishing link clicked but no password entered. Weak config found on a field device with no sign of abuse. Infected device that held no NFE credentials.

Severity	Impact	NFE response	Examples
S4 Low	Minimal impact; workaround available	Normal process / backlog	A policy slip with no sensitive data involved (e.g. a password in a private note, now changed). Phishing reported without engagement.

Things to weigh

- **Confidentiality, integrity, availability:** which of these are affected? The more, the higher the severity.
- **Affected surface:** customer sites and meters → shared servers (Nextcloud, mail, ERPNext, BookStack) → one account → one device.
- **Exploitability:** does it need one command, some effort, or rare conditions?
- **Visibility:** can everyone see it, people with specific access, or only you?
- **Privilege:** members of the Nextcloud `admins` group, server root and field-device admin accounts raise severity by one level.

When unsure, choose the **higher** severity. You can lower it after investigation.