Coordinated Vulnerability Disclosure Policy

Komax Group – Guidelines for reporting Security Vulnerabilities
Version: V1.4 | Last modified: 2026-08-04

Komax places a strong emphasis on the security of the systems, products, and services we develop and operate. It is possible that security vulnerabilities may still be discovered in Komax products, Komax-operated services, or in solutions operated on behalf of Komax.

We appreciate vulnerabilities being reported as early as possible, as this enables us to assess and implement appropriate mitigation measures in a timely manner to protect our customers and partners.

This document explains:

- how to report a vulnerability to Komax, and
- how Komax will handle vulnerability reports.

1. Reporting a vulnerability

If you believe you have found a security vulnerability in Komax products, Komax-operated services, or in solutions operated on behalf of Komax, please report it promptly via the channel below.

security@komaxgroup.com

If you would like a phone call, please include a telephone number where we can reach you.

2. What to include in your report (mandatory)

To help us verify and remediate the issue quickly, please provide:

- **Affected components:** Product/service name, affected versions, configuration details.
- **Vulnerability details & impact:** Describe the vulnerability and its potential impact.
- **Reproduction steps:** Clear step-by-step instructions to reproduce the issue (including environment details such as browser/version, scripts, timestamps, screenshots, etc.).
- **Contact details:** Email address or phone number so we can follow up (we also take anonymous reports seriously).
- **Optional:** Proof-of-Concept (PoC): Only if it is safe (i.e., does not damage, alter, or negatively impact the affected system or component), minimal, and necessary to demonstrate impact.

3. Rules for coordinated vulnerability disclosure

When handling vulnerabilities, please follow these rules to protect our customers, systems and products:

- **Do not share vulnerability details with third parties** until the issue has been resolved and disclosure has been coordinated with Komax.
- **Act responsibly and minimally:** only perform actions necessary to identify and validate the vulnerability.
- **Do not exploit the vulnerability** beyond what is required to prove its existence.
- **Do not access, modify, copy, or store** confidential data encountered during testing.
- **Avoid disruption:** do not degrade performance, cause outages, or interfere with production services.
- **Prohibited activities include (non-exhaustive):** physical attacks, denial-of-service (DoS/DDoS), social engineering, credential stuffing, phishing, malware deployment, or destructive testing.
- **Privacy and user experience must be protected:** avoid privacy violations, user disruption, or data deletion.

These guidelines are not an invitation to perform active, broad or intrusive scanning of Komax environments and/or Komax products. Komax monitors and assesses its systems and products together with its partners and service providers.

4. How Komax handles coordinated vulnerability disclosure

Within one business day of receiving your report, we will send an acknowledgement of receipt.

We aim to provide an initial assessment within:
One business day for critical vulnerabilities (CVSS 9.0-10.0), and up to three business days for all other reports, including:

- whether we were able to validate the report (or what we need to validate it), and
- an initial target date or plan for remediation (where possible).

Investigation and remediation

- Komax will investigate, triage severity, and assign the issue to the responsible teams.
- We may request additional details to reproduce the issue.
- We will coordinate fixes and mitigations and verify effectiveness.

Coordinated disclosure

- We aim to coordinate disclosure with the reporter where appropriate.

5. Good-Faith reporting
Security research conducted in accordance with this policy and within the defined scope is considered authorized by Komax. Komax will not initiate legal action against researchers who act in good faith, avoid privacy violations and service disruption, and promptly report discovered vulnerabilities through the channels defined in this policy. This protection does not apply to activities outside the defined scope, malicious actions, or conduct that causes harm to Komax, its customers, or third parties.

6. Security Information
Further security information is available at:

https://www.komaxgroup.io/security