OrangeHRM Vulnerability Disclosure Policy

OrangeHRM Open Source Application

Version 3.0
Effective Date: 6th March 2026

This Vulnerability Disclosure Policy ("Policy") establishes the terms under which external security researchers ("Researchers") may investigate and report potential security vulnerabilities affecting OrangeHRM Inc. ("OrangeHRM") products and services. The purpose of this Policy is to authorize responsible research, provide clear rules of engagement, and protect both Researchers and OrangeHRM by defining obligations and safe harbor provisions.

By conducting any security testing, research, or vulnerability reporting related to OrangeHRM open-source products or services, you acknowledge and accept that this Policy governs such activities.

Important Notice: Any security testing, scanning, or probing of OrangeHRM-hosted cloud services, demo instances, or customer environments is **strictly prohibited**. Only research conducted on self-hosted environments created from publicly available OrangeHRM open-source releases is authorized. Unauthorized activity may result in legal action.

1. Scope

This Policy applies exclusively to OrangeHRM open-source codebases, downloadable release packages, and Docker images made publicly available by OrangeHRM Inc.

Authorized scope: Security research on self-hosted instances deployed from official OrangeHRM open-source releases.

Not Authorized: Any form of scanning, probing, or testing of: OrangeHRM hosted demo environments (e.g., opensource-demo.orangehrmlive.com), Customer production environments, Third-party systems not owned or operated by OrangeHRM.

2. Eligibility and Reporting Procedure

Qualifying Vulnerabilities

- OrangeHRM accepts any vulnerability in the in-scope assets defined in Section 1 that demonstrates a realistic security impact on confidentiality, integrity, or availability, and is accompanied by a working proof of concept. Vulnerability class is not a limiting factor and are all eligible provided impact is demonstrated. Issues listed in "Non-Qualifying Vulnerabilities" are excluded regardless of class.

Non-Qualifying Vulnerabilities.

- Server, infrastructure, and deployment-level configuration.
- Deprecated features or functionality.
- Default credentials on the public demo instance.
- Missing best-practice hardening without demonstrable impact.
- Self-XSS, tab-nabbing, and attacks requiring physical device access.
- Username/email enumeration without an account takeover chain.
- Theoretical vulnerabilities with no working PoC.
- Social engineering, phishing, physical attacks, and DoS/DDoS.
- Issues in third-party services OrangeHRM does not control.
- Recently disclosed dependency 0-days within 14 days of public disclosure without proven impact.
- Vulnerabilities requiring an already-compromised privileged account.

Reporting Procedure

- All vulnerabilities must be reported to: ossecurity@orangehrm.com (PGP encryption recommended). Do not report issues through GitHub, social media, or public forums.
- To ensure secure communication, OrangeHRM strongly recommends encrypting all vulnerability reports using our public PGP key:
  - **PGP Key ID**: `AFA4F925FFC1D2C5`
  - **Fingerprint**: `DA77DCD55B79B11A1B2F680FAFA4F925FFC1D2C5`
  - Download: https://www.orangehrm.com/security/opensource/ohrm-vdp-pgp-key.asc
- Researchers should encrypt submissions to ossecurity@orangehrm.com using this key. Reports sent without encryption are accepted but not recommended.
- Reports must include the following sections:
  - Affected product version, release tag, or commit identifier
  - Title and description of the vulnerability
  - Proposed severity (This is optional, but if included in the report must be in CVSS 4.0)
  - Step-by-step instructions to reproduce the issue
  - Proof-of-concept - Videos, Images, PoC exploit codes
  - Potential impact assessment
  - Recommendations for remediation (optional)
- If multiple issues are discovered, they should be submitted together in a single, consolidated report, rather than being sent separately.

Use of AI for Vulnerability Reporting

- Vulnerabilities identified through the use of AI or LLM-based tools are required to be manually tested and verified in a self-hosted environment before reporting.
- AI tool usage for drafting, code review, or proof-of-concept development must be disclosed in the report.
- Failure to disclose AI tool usage, where subsequently identified, shall be treated as misrepresentation and addressed under the Rules of Engagement (Conduct Leading to Permanent Ban).

OrangeHRM will acknowledge receipt of reports within **7 business days** and communicate directly with the researcher regarding validation, remediation, and disclosure timelines.

3. Rules of Engagement

Researchers must adhere to the following requirements when conducting security testing:

- Use personal test environments (self-hosted) only (see OrangeHRM's Docker installation guide).
- Tests must be conducted on the latest available version of the OrangeHRM Open Source Application.
- Never test OrangeHRM demo, cloud, or production systems.
- Avoid automated vulnerability scanning tools (e.g., Nessus, Burp Suite) against the OrangeHRM infrastructure.
- Do not exfiltrate, modify, or destroy data.
- Do not conduct denial-of-service, brute force, phishing, social engineering or any physical attacks.
- Do not disclose vulnerabilities publicly or to third parties prior to disclosure by OrangeHRM via published Github Security Advisories.

Conduct Leading to Permanent Ban

1. Submitting fabricated, plagiarized, or AI-hallucinated reports.
2. Repeatedly submitting low-effort or duplicate reports after written warning.

538 Teal Plaza,Secaucus, New Jersey 07094, USA

3. Submitting the same vulnerability under multiple aliases or accounts.
4. Threatening, harassing, or pressuring OrangeHRM staff.
5. Bypassing the official program contact via GitHub, social media, public forums, or customers.

4. Disclosure Process and CVEs

OrangeHRM follows a structured process for handling reported vulnerabilities. The following principles apply to validation, remediation, and disclosure,

- Validated vulnerabilities will be addressed through GitHub Security Advisories.
- Please note that we will not publish advisories or request CVEs for "informative" level vulnerabilities.
- OrangeHRM will consider GitHub as its primary CVE Numbering Authority (CNA). Where applicable, OrangeHRM will request assignment of a CVE Identifier through GitHub's CVE issuance process.
- OrangeHRM requests that researchers allow up to **90 days** from initial submission for validation and release of a fix before any public disclosure.
- Public disclosure before the **90-day** remediation period without OrangeHRM's written consent constitutes a breach of this Policy.
- Researchers who responsibly report valid vulnerabilities will be credited in public advisories and release notes, unless they request anonymity.

5. Legal Safe Conduct

OrangeHRM will not initiate legal proceedings against Researchers who conduct security testing in full compliance with this Policy. This assurance does not apply to any activity that falls outside the defined scope or violates the Rules of Engagement.

- Activities carried out in accordance with Section 3 are deemed authorized.
- OrangeHRM waives any claims under the Computer Fraud and Abuse Act (CFAA) or equivalent laws where research is conducted within the defined scope of this Policy.

If unsure about an activity's compliance, suspend testing immediately and contact ossecurity@orangehrm.com for clarification.

6. Confidentiality

Researchers must treat all vulnerability information as confidential and may not disclose details to third parties without OrangeHRM's prior written consent. Public disclosure outside the parameters of Section 4 constitutes a breach of this Policy. OrangeHRM will treat researcher submissions as confidential and will not disclose identifying information without consent, except as required by law.

7. Data Protection

During testing and reporting, researchers must avoid accessing, storing, or transmitting personal data. Any access to personal or sensitive data outside the scope of this Policy is unauthorized and not protected under Section 5. If inadvertent access to personal or sensitive data occurs, Researchers are required to:

1. Cease testing immediately.
2. Notify OrangeHRM without delay.
3. Not retain, use, or disclose such data.

538 Teal Plaza,Secaucus, New Jersey 07094, USA

8. Intellectual Property

All intellectual property rights in OrangeHRM software, systems, and related materials remain the sole property of OrangeHRM Inc. No license or right is granted to Researchers except as expressly stated in this Policy.

9. No Bug Bounty Program

OrangeHRM does not offer monetary rewards or bug bounties. All submissions are voluntary and made without expectation of compensation. Valid reports may be publicly acknowledged unless anonymity is requested.

10. Limitation of Liability

To the fullest extent permitted by law, OrangeHRM shall not be liable for any damages, losses, or claims arising from or related to security research conducted under this Policy. Researchers acknowledge that OrangeHRM reserves the right to pursue legal remedies for any activity conducted outside the authorization defined by this Policy.

11. Consequences of Policy Breach

Unauthorized activities; including testing outside the scope, scanning OrangeHRM infrastructure, or premature disclosure, may result in legal action under the Computer Fraud and Abuse Act (CFAA) or similar laws.

12. Governing Law

This Policy shall be governed by and construed in accordance with the laws of the State of New Jersey, United States of America, without regard to its conflict of law provisions. Any disputes shall be subject to the exclusive jurisdiction of the state and federal courts located in New Jersey.

13. Entire Agreement

This Policy constitutes the entire agreement between Researchers and OrangeHRM with respect to vulnerability disclosure activities. It supersedes any prior agreements or understandings, written or oral, relating to the same subject matter. OrangeHRM reserves the right to amend this Policy at any time. Any revisions will be published with a revised effective date, and continued research or submissions after such publication will constitute acceptance of the updated Policy. If any provision of this Policy is held invalid, the remainder shall continue in full force and effect.

538 Teal Plaza,Secaucus, New Jersey 07094, USA