Vulnerability Disclosure Policy

1. Overview

Ubiquiti is committed to the security of our products and the customers who rely on them. We welcome responsible disclosure of security vulnerabilities and may choose to collaborate with security researchers to investigate and remediate valid issues in a coordinated manner.

This policy describes how to report security vulnerabilities and how Ubiquiti handles disclosures.

2. Reporting a Vulnerability

Security vulnerabilities may be reported to Ubiquiti through one of the following channels:

- HackerOne: https://hackerone.com/ui
- Email: security@ui.com

Communications regarding a report should be conducted in English through the channel used to submit the report. Reports should include the affected product, service and firmware or software version, a description of the vulnerability and its potential impact, and steps to reproduce the issue.

3. Scope & Definition

For the purposes of this policy, a vulnerability is strictly limited to a technical weakness that directly impacts the confidentiality, integrity, or availability of (i) hardware, firmware, or software developed and distributed by Ubiquiti (the "Product Vulnerability) or (ii) customer-facing cloud services developed and operated by Ubiquiti, including the web application and the cloud hosting service that form part of such services (the "Cloud Vulnerability"). This policy does not apply to Ubiquiti's corporate infrastructure or any third-party products/services, all of which are explicitly excluded from scope. Product Vulnerabilities may be considered for CVE assignment and public disclosure in accordance with Sections 5 and 6. Cloud Vulnerabilities may be reported to Ubiquiti under this policy and may be investigated, validated, and remediated by Ubiquiti.

4. Secure Communication

Ubiquiti's PGP public key is available at: https://ui.com/security/pgp-key

5. Vulnerability Handling & Disclosure

Ubiquiti evaluates submitted reports based on severity and operational capacity. Ubiquiti reserves the right, in its sole discretion, to determine whether to investigate, validate, or patch any reported vulnerability, and whether to assign a CVE identifier to any reported Product Vulnerabilities. Ubiquiti aims to acknowledge receipt of a report within ten (10) business days. Analysis, remediation, and disclosure timelines vary with the severity and complexity of each

© 2026 Ubiquiti Inc. All rights reserved.

issue. The substance and timing of any disclosure of Product Vulnerabilities is determined in Ubiquiti's sole discretion, however, Ubiquiti will seek to coordinate the timing of public disclosure with the reporter where possible.

6. CVE ID Assignment and Publication

If Ubiquiti, in its sole discretion, validates a report as a Product Vulnerability eligible for CVE assignment, it may reserve a CVE ID and share it with the reporter. The CVE Record is typically published when the corresponding security advisory is released. Ubiquiti reserves the right to control all public communications regarding reported vulnerabilities. Reporters are expected to keep the CVE ID and all vulnerability details strictly confidential unless and until Ubiquiti publicly releases an advisory. Ubiquiti does not publicly discuss vulnerability details, proof-of-concept material, or the status of individual reports prior to publication of an advisory. Upon publication, Ubiquiti may publicly discuss the information contained in the advisory and the associated CVE Record, including affected products and versions, a general description of the vulnerability, its severity, and available fixes or mitigations. Reporters may be publicly credited in the advisory with their consent.

7. Relationship to the Bug Bounty Program

This policy is distinct from any bug bounty programs operated by Ubiquiti. Submission of a report under this policy does not guarantee, create eligibility for, or entitle the reporter to any financial compensation or bounty award.

8. Public Advisories

Security advisories and vulnerability disclosures are published at: https://community.ui.com/releases?security-updates

9. Researcher Expectations

We ask that security researchers:

- Avoid testing that degrades service availability or impacts customers
- Do not publicly disclose vulnerabilities prior to Ubiquiti's public advisory or explicit authorization
- Act in good faith and in accordance with applicable laws

10. Legal Disclaimers & No Warranty

This policy is provided on an "as is" basis and does not create any binding legal agreement, contract, representation, or warranty between Ubiquiti and any third party. Participation in this program is entirely voluntary. Ubiquiti reserves the right to modify, suspend, or terminate this policy at any time without notice. To the maximum extent permitted by law, Ubiquiti disclaims all liability for any expenses, damages, or losses incurred by any party in connection with this policy or the submission of vulnerability reports.

Last Updated: August 25, 2026

© 2026 Ubiquiti Inc. All rights reserved.