Product Cyber Security Vulnerability Disclosure Policy

Policy

Husqvarna Group

Husqvarna Group Global

1 PURPOSE & SCOPE

This policy defines how external parties can report cybersecurity vulnerabilities in Husqvarna Group products and services, and how Husqvarna Group manages such disclosures.

- Enable early detection of vulnerabilities
- Support coordinated vulnerability disclosure
- Ensure compliance with relevant regulations such as the EU Cyber Resilience Act (CRA)
- Protect customers, users, and the company

This policy applies to:

- Products developed or maintained by Husqvarna Group
- Vulnerabilities that are either exploitable or have potentially been exploited
- External researchers, customers, partners, and suppliers reporting vulnerabilities
- Complete product lifecycle stages (development, operation, maintenance)

2 DESCRIPTION

2.1 Reporting a Vulnerability

We encourage responsible disclosure of vulnerabilities from security researchers, customers, partners, suppliers and public.

Contact Channels

- Web form: https://cybersecurity.husqvarnagroup.com
- Email: productsecurity@husqvarnagroup.com

2.2 Our Commitment

We support good-faith cybersecurity research. Husqvarna Group will not tolerate any retaliation as a result of reporting, provided such reporting is done in good faith or with a reasonable belief. When you report a vulnerability, we will:

- Acknowledge receipt
- Assess and validate the report
- Work to remediate the issue in a timely manner
- Coordinate public disclosure where appropriate

We prohibit exploiting vulnerabilities for any gain that is not contributing to the goal of this policy.

2.3 Vulnerability Handling Principles

All reported vulnerabilities will be:

- Reviewed and validated
- Assessed for impact and severity
- Tracked and managed through remediation lifecycle

2.4 Coordinated Vulnerability Disclosure (CVD)

We follow a coordinated disclosure process:

- Public disclosure occurs only after:
  - Fix or mitigation is available, or
  - Risk is sufficiently reduced
- Communication aligned with:
  - Customer protection

- Legal and regulatory requirements

- We request that reporters
  - Avoid public disclosure until coordination is complete
  - Share findings confidentially

2.5 Communication and Public Disclosure

On a vulnerability is resolved or mitigated, we may publish, where applicable:

- Security advisories
- Vulnerability disclosures (e.g., CVEs)
- User notifications of actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, including where necessary, of any risk mitigation and corrective measures

We will credit the reporter if desired.

2.6 Regulatory Reporting

Where required under the EU (2024/2847) Cyber Resilience Act (CRA) and other applicable regulations, we will:

- Submit an early warning notification of any actively exploited vulnerability or severe incident to the designated authority or coordinator (e.g., for CRA, the CSIRT and ENISA)
- Meet mandatory legal timelines (e.g., for CRA, the timelines set out in Article 14)
- Cooperate with relevant authorities
- Notify impacted users

2.7 Third-Party Vulnerabilities

If a report affects third-party components or open-source components integrated into Husqvarna Group products:

- We will notify the relevant supplier without undue delay, and address and remediate vulnerability in accordance with applicable vulnerability handling requirements
- Disclosure may depend on upstream remediation timelines

3 Policy Updates and Contact

This policy will be reviewed periodically and updated as needed to reflect changes in products and services, regulatory changes, evolving best practices, and lessons learned.

Email: productsecurity@husqvarnagroup.com