

DAKTRONICS VULNERABILITY DISCLOSURE POLICY

1. Purpose.

Daktronics is committed to protecting our customers, partners, and products through responsible vulnerability management. We recognize the valuable role that security researchers, customers, and the broader security community play in identifying vulnerabilities that may affect Daktronics products and services.

This Vulnerability Disclosure Policy (VDP) provides a process for reporting potential security vulnerabilities and describes how Daktronics receives, evaluates, remediates, and coordinates disclosure of verified issues.

2. Scope.

This policy applies to Daktronics:

- Hardware products
- Control systems
- Embedded devices and firmware
- Stand-Alone Software applications
- Cloud-hosted and associated web services
- Mobile applications
- Network-connected display systems

Reporters should report third-party vulnerabilities directly to the appropriate vendor.

3. Safe Harbor.

Daktronics authorizes good-faith security research conducted within the boundaries of this policy.

Daktronics will not pursue legal action against security reporters who:

- Comply with this policy
- Act in good faith
- Avoid causing harm to customers or Daktronics
- Promptly report discovered vulnerabilities
- Do not violate applicable laws

Activities outside the scope of this policy, including unauthorized access, data theft, service disruption, or privacy violations, are not authorized and will be reported to the appropriate authorities

4. Rules of Engagement.

Reporting Parties must:

- Make every effort to avoid impacting product availability.
- Test only what is necessary to confirm the existence of a vulnerability.
- Immediately stop testing if sensitive customer information is encountered.
- Report vulnerabilities promptly.
- Maintain confidentiality until coordinated disclosure has been completed.

Reporting Parties must not:

- Access, modify, or delete data for which you are not authorized.
- Access or modify equipment for which you are not authorized.
- Attempt denial-of-service testing.
- Conduct physical intrusion activities.
- Use social engineering, phishing, or impersonation techniques.
- Install malware or persistent software.
- Exploit vulnerabilities beyond what is required for verification.
- Publicly disclose vulnerabilities before coordination with Daktronics.

DAKTRONICS VULNERABILITY DISCLOSURE POLICY

5. Out-of-Scope Activities.

The following are generally outside the scope of this policy:

- Physical security testing
- Disclosure of previously known vulnerabilities without additional findings
- Findings that require unrealistic attack preconditions
- Vulnerabilities in third-party products not controlled by Daktronics

Reporters should report third-party vulnerabilities directly to the appropriate vendor.

6. Reporting a Vulnerability.

Reports for each vulnerability should include, whenever possible:

Product Information

- Product name
- Model number and/ or Part Number
- Firmware, software, or hardware version

Vulnerability Details

- Description of the issue
- Potential security impact
- Affected component

Reproduction Information

- Step-by-step instructions
- Proof-of-concept information
- Screenshots or log files
- Network capture data (if applicable)

Reports may be submitted through: [The Daktronics Vulnerability Reporting Form](#), or by sending an Email to: ssirt@daktronics.com**

***Note: Daktronics does not support PGP-encrypted email communications. Please do not include sensitive or confidential information in your vulnerability report or email correspondence. If your report contains sensitive information, indicate this in your submission, and a Daktronics representative will contact you to establish a secure method for information sharing.*

7. Daktronics Response Commitments.

Except for circumstances where applicable laws may require shorter response targets, Daktronics aims to:

Activity	Target
Acknowledgement	Within 3 business days
Initial triage	Within 10 business days
Ongoing communication	At least every 30 days
Remediation assessment	As risk warrants
Coordinated disclosure	Upon availability of mitigation

Complex issues may require additional investigation time. Response times are objectives rather than contractual commitments.

8. Vulnerability Handling Process.

Upon receiving a report, Daktronics SSIRT will:

- Acknowledge receipt.
- Validate the reported issue.
- Assess severity and exploitability.
- Determine affected products and customers.

DAKTRONICS VULNERABILITY DISCLOSURE POLICY

- Develop mitigation or remediation plans.
- Coordinate internal engineering response.
- Determine notification requirements.
- Publish advisories where appropriate.
- Coordinate public disclosure.

9. Coordinated Disclosure.

Daktronics follows coordinated vulnerability disclosure principles.

Daktronics requests that reporters:

- Allow a reasonable period for validation and remediation.
- Avoid public disclosure before mutually agreed release milestones.
- Coordinate disclosure timing with Daktronics.

When appropriate to protect customers and infrastructure, Daktronics may coordinate with:

- Customers
- Industry partners
- CERT/CC
- VINCE
- CISA
- ENISA
- CVE Numbering Authorities (CNAs)
- National cybersecurity agencies

10. Public Advisories and CVEs.

For significant vulnerabilities, Daktronics may:

- Publish a security advisory.
- Request CVE assignment.
- Provide mitigation guidance.
- Notify affected customers.
- Coordinate disclosures through VINCE, CERT/CC, or governmental authorities when necessary.
- Any other action that Daktronics reasonably determines to be appropriate

11. Compensation Policy.

Daktronics currently does not offer financial compensation or bug bounty rewards.

12. Legal Notice.

Nothing in this policy grants authorization to:

- Access Daktronics systems or third-party data without permission
- Exceed the scope defined within this policy.
- Violate laws or regulations.
- Access data unrelated to vulnerability verification.

Reporters remain responsible for complying with applicable laws.

13. Policy Updates.

Daktronics may revise this Vulnerability Disclosure Policy at any time. Updated versions will be published on the Daktronics website.

DAKTRONICS VULNERABILITY DISCLOSURE POLICY

Revision History

Version	Date	Notes
1.0	09/15/2026	Initial Document

Policy Owner: Daktronics Solution Security Incident Response Team (SSIRT)

Contact: ssirt@daktronics.com