

Security Vulnerability Disclosure Policy

Overview

NETIKUS.NET welcomes reports from security researchers and users who discover potential vulnerabilities in our products or web properties. We are committed to investigating all responsibly disclosed reports and working with researchers to address legitimate security issues in a timely manner.

Scope

We distinguish between three categories of security reports:

EventSentry Product

Vulnerabilities affecting EventSentry — including the agent, web console, and supporting services — are our highest priority. We treat product vulnerabilities with the utmost seriousness given that EventSentry is deployed in enterprise security environments where the integrity of the software is critical to our customers' operations. Reports in this category will receive a response within 2 business days and we will provide regular updates throughout our investigation.

Customer Portal (store.netikus.net)

Our online store and customer portal handles account authentication and customer data. We treat vulnerabilities affecting this property with elevated priority. Reports in this category will receive a response within 2 business days.

Web Properties

Vulnerabilities affecting our remaining public-facing web properties are reviewed on a best-effort basis. While we take all reports seriously, the risk profile of these sites differs from that of our core product and customer portal. Our web properties include:

- netikus.net
- eventsentry.com
- system32.eventsentry.com
- myeventlog.com

Reports in this category will receive a response within 5 business days.

How to Submit a Report

Please submit vulnerability reports to support@netikus.net and include the following information where possible:

- A description of the vulnerability and its potential impact
- The affected component (EventSentry product, customer portal, or web property)
- Steps to reproduce the issue
- Any supporting evidence such as screenshots or proof-of-concept code

We ask that you do not publicly disclose the vulnerability until we have had a reasonable opportunity to investigate and, where necessary, issue a fix.

Compensation

NETIKUS.NET does not operate a formal bug bounty program and does not offer monetary compensation for vulnerability disclosures. Security research is handled directly by our engineering team. Researchers who report valid vulnerabilities in EventSentry or our customer portal will be acknowledged in our security advisories, unless they prefer to remain anonymous.

Coordinated Disclosure

We aim to resolve confirmed product vulnerabilities within 90 days of a validated report. We will keep the reporting researcher informed of our progress and will coordinate the timing of any public disclosure with them where possible.

Good Faith

We ask that researchers act in good faith and avoid accessing, modifying, or exfiltrating data beyond what is necessary to demonstrate the vulnerability. We commit to the same good faith in return — we will not pursue legal action against researchers who follow this policy.