Nice Coordinated Vulnerability Disclosure Policy / Public Policy

Nice takes the security of its products and digital services seriously. If you believe that you have identified a security vulnerability affecting a Nice product or service, please report it to us. This policy explains how to submit a report, the information that helps us assess it, and what you may expect from us.

How to report

1. email security@niceforyou.com. Use a clear subject line, for example: “Security vulnerability report – [product or service]”.
2. Do not include unnecessary personal data or third-party confidential information. If you would like to receive updates, provide a reliable contact method.

What to include

1. the affected product or service, or a description sufficient to identify it; model, firmware/software version, application version or service URL may be provided where known;
2. a clear description of the suspected vulnerability and, where known, its potential impact;
3. the steps required to reproduce the issue and, where available, a proof of concept; these items are helpful but are not required where the reporter cannot provide them;
4. the conditions required for exploitation, including the attack vector and privileges required, where known;
5. any information indicating that the vulnerability may already be actively exploited; if this cannot be determined, select or state “unknown/not observed”.

What you can expect from us

1. We aim to acknowledge receipt within 3 business days. The acknowledgement includes the case ID and confirms receipt only; it does not constitute validation of the reported vulnerability.
2. We aim to provide an initial assessment or status update within 10 business days.
3. Where the investigation remains open and you have provided contact details, we aim to provide a status update at least every 30 days, unless legal, security or confidentiality reasons prevent us from sharing particular information.
4. These are service targets for communication with reporters. They do not replace or modify any statutory reporting deadlines applicable to Nice.

Coordinated disclosure

Please allow Nice reasonable time to investigate and, where appropriate, remediate the reported issue before making it public. We will seek to coordinate any disclosure with you, taking into account the severity of the vulnerability, the availability of corrective measures, the protection of users and any applicable legal obligations. Where appropriate and with your consent, Nice may publicly acknowledge your contribution.

Good-faith security research

If you conduct security research in good faith and comply with this policy, Nice will not initiate or support legal action against you solely in connection with that research. This commitment applies only to systems and activities within the scope of this policy and within Nice's authority. It does not bind third parties and does not authorize conduct that is unlawful or exceeds the limits set out below.

Research requirements

1. test only products, accounts, devices or systems that you own or are expressly authorized to test;
2. avoid privacy violations and minimize access to personal data or confidential information;
3. stop testing and notify us promptly if you access data that is not necessary to demonstrate the vulnerability;
4. do not retain, alter, delete, download, copy, disclose or otherwise use data belonging to Nice, its users or third parties, except for the minimum information strictly necessary to document the vulnerability;
5. do not establish persistent access, perform social engineering, threaten or extort, disrupt services, or conduct denial-of-service or volumetric testing;
6. do not exploit the vulnerability beyond what is strictly necessary to demonstrate it; and
7. allow reasonable time for investigation and remediation before public disclosure.

Scope

This policy applies to Nice products with digital elements that are within their declared support period, including associated firmware, software, mobile applications and cloud services, and to websites or digital services operated directly by Nice. Reports concerning unsupported products may still be submitted and will be assessed on a case-by-case basis, without creating a commitment to provide a corrective update.

Out of scope

1. systems, products or services operated exclusively by third parties, unless Nice has expressly authorized their inclusion;

2. physical attacks, social engineering, phishing or attacks against employees, contractors, customers or suppliers;
3. denial-of-service, distributed denial-of-service or tests that may impair availability or performance;
4. automated testing that generates excessive traffic or interferes with normal service operation;
5. access to, alteration, destruction, retention, extraction or disclosure of data beyond what is strictly necessary to demonstrate the vulnerability; and
6. testing of products, accounts, devices or systems that you do not own and are not authorized to test.

Reports involving third-party components

If a report concerns a third-party component integrated into a Nice product, please report it to Nice. We will assess the issue and, where appropriate, coordinate with the relevant component manufacturer, supplier or maintainer in accordance with our internal vulnerability-handling process.

No bug bounty commitment

This policy does not create a bug bounty programmed or an entitlement to payment, reward or other compensation. Any recognition or reward must be expressly agreed by Nice in writing.

Personal data

Personal data provided with a vulnerability report will be processed only as necessary to receive, assess, investigate and manage the report, communicate with the reporter, protect Nice and its users, and comply with applicable legal obligations. The applicable privacy notice under Regulation (EU) 2016/679 is available on the security-reporting page.