FORESCOUT

Forescout Security Disclosure and Report

Why We Care

Forescout is committed to ensuring the safety and security of our customers. We care deeply about protecting our customers' and employees' data, as well as designing and testing our products and their supply chain dependencies.

In this document, you will find information on how to report possible security bugs or vulnerabilities in our products. As builders of security products, we understand the importance of reporting and investigating potential security issues and encourage researchers to report any security issues in our infrastructure, products and websites.

Scope

The activities that are within the scope of the policy are here:
https://hackerone.com/forescout_technologies.

All other activities that are not listed as "in scope" are deemed to be out of scope. Out of scope includes customer production environments and customer information and data, unless approved by the customer.

How to Submit a Vulnerability

There are two ways you can report a vulnerability.

1. Hackerone

You may join our HackerOne program to report issues about our products or websites, and get rewarded for finding issues that are in scope as detailed at https://hackerone.com/forescout_technologies. To do so, you can request to be added to the HackerOne program.

2. Email to Forescout's Product Security Team

The other way is to report a vulnerability directly by emailing Forescout's Product Security Team at security@forescout.com. Submitting the vulnerability directly to Forescout will not entitle you to a bounty reward as we currently do not have a program to administer the details of payment.

When you send an issue to security@forescout.com, please provide the details of the vulnerability in English and keep the following in mind.

- Reports should include a proof of concept code or other proofs.
- Reports that include only crash dumps or another automated tool output will most likely not be accepted.
- Reports that include products not on the covered list will most likely be ignored.
- Include how you found the bug, the impact and any potential remediation.
- Provide any plans for public disclosure. We would like to coordinate any public disclosure of the vulnerability with you.
- Include your contact details

Preference, Prioritization and Acceptance Criteria

What you can expect from us:

- A timely response to your email (usually within 72 hours).
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.
- Researchers who submit a vulnerability report to us will be given full credit on our website once the submission has been accepted and validated by our product security team.
- Forescout may not release the exact details of vulnerabilities.
- Forescout will announce vulnerabilities on our customer product support portal
- Forescout will not publicly announce security vulnerabilities until fixes are publicly available.
- For critical-risk, high-impact vulnerabilities, Forescout may contact customers that are especially vulnerable in order to recommend mitigations in cases where a fix is not yet available.

Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Preferences for Public Notification

If applicable, Forescout will coordinate public notification of a validated vulnerability with you. When possible, we prefer that our respective public disclosures be posted simultaneously. In order to protect our customers, Forescout requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to and addressed the reported vulnerability and informed customers if needed. We appreciate your cooperation in the matter.

Coordinated Vulnerability Disclosure Policy for Forescout Research

In cases where our dedicated research team discovers security vulnerabilities in third-party vendors' software, hardware or products, we will make a good-faith effort to privately contact the third-party vendor with the details of the findings and give them a chance to fix the issues, before releasing the research to the public. We believe in coordinated disclosure practices.

After finding a vulnerability in a third-party vendor product and rating it for severity and impact, we will:

1. *Keep any communication confidential regarding the vulnerability until the completion of the disclosure process.*

2. *Attempt to contact the appropriate product vendor and request an email security contact to share sensitive details about the findings. We will check for the existence of public bug bounty listings, vulnerability disclosure policy or any security contacts for the vendor to use accordingly.*

3. *Request a Common Vulnerabilities and Exposures (CVE) ID from MITRE.org. The vulnerability details will not be made public immediately and the CVE ID will remain marked as RESERVED until the details are populated.*

4. *If vendor does not acknowledge the issue and we deem its impact is critical enough, we will send a notification to relevant computer emergency response teams (CERTs) 15 days after the first attempt at contacting the third-party vendor.*

In keeping with CERT best practices, we will prepare and publish an advisory detailing the vulnerability after one of the following events: either the vendor publicly addressed the issue with a fix or workaround, or at least 90 days pass after initial attempts at disclosure, barring extenuating circumstances, whichever happens first.

This advisory will be made available to the general public via Forescout's website. It is likely there may also be some media interest, depending on the details of the findings.

Publishing can include a conference presentation, a blog entry or a report (e.g., PDF), etc.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com