OKTA VULNERABILITY DISCLOSURE POLICY

A. OKTA SECURITY + RESEARCHER COLLABORATION

We believe community researchers play an integral role in maintaining Okta as a secure service and helping to protect our customers and their data. Our aim is to do what's best for our users, customers, partners, and the general health of the Internet.

We appreciate all security submissions from the research community and strive to respond in an expedient manner. We will investigate legitimate reports and do our best to quickly fix any identified issues. Our investigation panel consists of members from the Okta Security Team.

Please submit your report to our team as soon as you believe you have found a security vulnerability. All submissions must meet the terms of this Vulnerability Disclosure Policy ("policy").

- If you would like to publish your findings, the coordinated disclosure terms below apply and you must submit the report directly to us at psirt@okta.com, preferably using GPG encryption (key).
- If you would like to be rewarded, the Bugcrowd's standard disclosure terms apply, and you must submit via Bugcrowd to be rewarded for your submission. For more information, visit our bug bounty programs for Auth0 and Okta.

B. PROGRAM AND SCOPE

In-scope and out-of-scope targets are described in our Bugcrowd program terms for Auth0 and Okta. The same scope applies whether you are submitting a finding under standard disclosure terms through Bugcrowd or our coordinated disclosure terms (described below).

Please understand that third-party services not owned by Okta (such as apps integrated as part of the Okta Integration Network) are not eligible. While we strive for secure integrations, we cannot ensure that our policies apply to the services of other companies.

C. EVALUATION AND EXPECTATIONS

Explain the vulnerability impact

We base all payouts on impact - when in doubt, the question always comes down to the potential impact of the vulnerability (i.e., what can actually be done with the vulnerability and what is the consequence to Okta). If you can demonstrate why a finding has significant impact, then please submit that information.

For example, if the vulnerability you identify is that you are a limited admin and have the ability to see user logs not assigned to your user role, then we would examine the impact of this exploit. If the impact is high and allows you to compromise another aspect of the service, we ask that you detail the full exploit chain and report. However, if the only impact results in reading logs, then there is no need to report it because it would be classified as a business logic read issue.

Chaining bugs

Chaining of bugs is not frowned upon in any way: we love to see clever exploit chains! However, if you have managed to compromise an Okta-owned server, we do not allow for escalations such as port scanning internal networks, privilege escalation attempts, attempting to pivot to other systems, etc.

If you get this level of access to a server, please report your findings to us immediately and we will reward you with an appropriate bounty, taking into full consideration the severity of what could be done. Ex.: Chaining a CSRF vulnerability with a self XSS? Nice, report it to us! Using AWS access key to dump sensitive info? Not cool (and against our policy).

Reporting

To prioritize security and respect your research, we ask that you:

- Contact us immediately if you come across any customer, user, or personal data. Do not view, alter, copy, save, store, transfer, download, or access this data and immediately delete any local data upon reporting the vulnerability to us.
- Write clear and detailed reports so we can verify the vulnerability.
- Give us a reasonable amount of time to respond to the issue and respect our standard disclosure terms if you report via Bugcrowd or our coordinated disclosure terms (below) if you choose not to receive a bounty reward and publish your findings.
- Do not modify our data, content, or any customer or user's data or content.
- Only use your own account or test accounts for security research purposes.
- Please be respectful of our existing application and do not test for spam, use automated vulnerability scanners, social engineering, or denial of service issues.
- Act in good faith to avoid privacy violations, destruction of data, and interruption or degradation of our services (including denial of service).

Valid reports

We ask that you write clear and concise reports to enable us to make a determination. Please make sure to include your methodology, step-by-step, and only submit after you verify your bug.

D. LEGAL SAFE HARBOR

If you comply with the terms of this policy when reporting a potential security issue to us, whether directly or through Bugcrowd, we will not pursue civil action or file a complaint with law enforcement for accidental, good faith violations of this policy. We consider activities conducted consistent with this policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act. We will not bring a Digital Millennium Copyright Act claim against you for circumventing the technological measures we have used to protect the applications in scope.

If legal action is initiated by a third party against you and you have complied with this policy, including any applicable program rules or other incorporated terms, Okta will take steps to make it known that your actions were conducted in compliance with this policy.

E. COORDINATED DISCLOSURE TERMS

Okta takes a responsible disclosure stance for vulnerabilities submitted to us directly. If you disclose a bug to us directly, then you agree to give us at least 90 days to investigate the bug and fix the issue before making any public disclosure or sharing the information with any other person or third party.

We will strive to fix this, allow disclosure within industry standard timelines and may extend this period as needed based on the vulnerability, complexity, and potential effects. If for some reason, we need to extend this timeline, we're happy to work together with you to determine whether to proceed with publication and appreciate any prior notice. We request that you run your publication content by us in advance of sharing it publicly. If the vulnerability is novel or impactful, we intend to publicly share details around the vulnerability and coordinate with you on reasonable timing. Reasonable response times to fixing vulnerabilities help create a safer Internet for everyone.

If you choose to be compensated for your bug and you submit your findings via our programs on Bugcrowd, then you may not disclose the bug publicly or to any other person or third party, without prior explicit authorization. These submissions will be governed by Bugcrowd's Standard Disclosure Terms and the bounty rewards payment you receive is subject to the terms therein.

F. PAYOUTS

For bug bounty rewards, the following terms apply:

- We will only reward the individual that is the first to report a vulnerability to us and will not reward informative reports.
- Violation of this policy, disclosure of the vulnerability subject to the coordinated disclosure terms or any other public disclosure of the vulnerability prior to resolution may result in canceling a pending reward.
- We reserve the right to disqualify individuals from the program for disrespectful, disruptive, or otherwise inappropriate behavior.
- We reserve the right to ask you for more details or updates to your report to make a determination.
- We reserve the right to determine the amount of a reward and whether it should be granted, including paying more or less based on the vulnerability.
- All rewards are based on the security risk and impact of the issue.

Please visit our Bugcrowd program policy for additional terms. For more information, visit our bug bounty programs for Auth0 and Okta.

G. OTHER TERMS

The following terms apply to this policy and to any rewards paid to you for disclosing vulnerabilities through Bugcrowd:

- The "terms applicable to all research" in the Vulnerability Disclosure Policy Supplemental Terms, including the sections: (i) Okta's Rights to Fully Exploit Submissions, (ii) Trademark, (iii) Confidentiality, (iv) Limitation and Liability, and (v) Miscellaneous are incorporated within this policy and apply to all research and reports you submit.
- You must comply with all applicable laws and must not compromise or disrupt any data that is not your own. You are responsible for any tax implications for bounty rewards depending on your country of residency and citizenship. There may be additional restrictions on your ability to submit depending upon your local law.
- Reports from individuals who we are prohibited by law from paying are ineligible for bounty rewards. Employees and their family members are not eligible for bounty rewards. You must be at least 18 years old or have reached the age of majority in your jurisdiction of primary residence and citizenship to be eligible to receive any bounty reward.
- We may modify the terms of this program or terminate this program at any time. The decision as to whether or not to pay a reward has to be entirely at our discretion. We won't apply any changes we make to these program terms retroactively.
- Okta can use and share your findings and submissions in any way for any purpose.

Thanks for submitting a vulnerability report and collaborating with us to improve security!

Last updated: August 26, 2024