kandji

Kandji Responsible Disclosure Policy

Classification :: Public

Revision History

Version	Revision Date	Revised By	Approved By	Change Log
1.0	8/01/2020	VP Architecture	Chief Operating Officer	Initial Version
1.1	8/01/2021	VP Architecture	Chief Operating Officer	Annual Review
1.2	8/01/2022	GRC Analyst	VP Security and Trust	Annual Review
2.0	8/01/2023	VP Security and Trust	Chief Technology Officer	Annual Review, Added Kandji Vulnerability Research and Disclosure Principles, Coordinated Vulnerability Disclosure (CVD) Policy, Commitment to Researchers, All Vulnerabilities

We believe community researchers play an integral role in maintaining Kandji 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 Kandji 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").

Kandji's Vulnerability Research and Disclosure Principles

We believe in strengthening defense by democratizing access to attacker tooling and knowledge. One of Kandji's unique strengths is our deep knowledge of how attackers work. Releasing public exploit code and novel research is core to our mission to close the security achievement gap.

Public disclosure of vulnerabilities is a critical component of a healthy cybersecurity ecosystem. Kandji's practices and advocates for timely public disclosure of vulnerabilities across both third-party products and our own systems and solutions. This includes vulnerabilities we independently discover in macOS systems and software. Through transparent, open, and timely vulnerability disclosures, Kandji helps the entire internet protect and defend those assets and services critical to modern civilization.

In today's threat landscape, organizations need timely information about risk in order to make educated choices about protecting their networks — especially during active attacks. Our vulnerability disclosure policy includes explicit provisions for speeding up public disclosure in cases where exploitation has been observed in the wild. Vendors often (understandably) act to protect their own businesses and reputations when there are security issues in their products that introduce risk into their downstream customers' environments. When we know about exploitation in the wild, or when we believe that threat actors may be covertly weaponizing non-public vulnerabilities, our priority is to make customers and the community aware of that risk so they may take action to protect their organizations.

Reporting a Potential Security Vulnerability

For the security of our users and service, we ask that you do not share details of the suspected vulnerability publicly or with any third party.

Please report the details of any suspected or detected vulnerabilities with Kandji by completing the submission form on this page, or by emailing vdp@kandji.io, including the following information:

- Provide clear and reproducible steps that demonstrate the vulnerability exists
- Avoid privacy violations, destruction of data, and interruption or degradation of our services.
- Do not modify or access data that does not belong to you.

Coordinated Vulnerability Disclosure (CVD) Policy

In keeping with standard industry practices around Coordinated Vulnerability Disclosure (CVD) (such as CERT/CC's, Google's, ZDI's) Kandji will typically prepare and publish advisories detailing newly discovered vulnerabilities approximately 90 days after our initial attempts at private disclosure, barring extenuating circumstances (including those outlined below which may warrant different disclosure guidelines). These advisories will be made publicly available via Kandji's blog and social media. Depending on the details of the findings, there may also be media engagement.

While coordinated vulnerability disclosure can differ from bug to bug depending on a wide range of circumstances, Kandji's primary concern is getting vulnerabilities fixed and making affected parties aware of the risks associated with vulnerabilities. In keeping with the principles outlined above, Kandji has identified several common types of vulnerabilities, each of which warrants slightly different disclosure guidelines.

Please note, technical vulnerabilities often involve undefined behavior and unexpected interactions. Therefore, Kandji may modify the timeline for disclosure at our sole discretion due to unique or unpredictable elements of that specific vulnerability.

Authorization

If you make a good faith effort to comply with this document during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and Kandji will not recommend or pursue legal action related to your research.

Guidelines

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential privacy or security vulnerability.

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems

Once you've established that a vulnerability exists, or encounter any sensitive data (including personally identifiable information, financial information, proprietary or trade secret information of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Prohibited Actions

While we encourage you to discover and report to us any vulnerabilities you find in a responsible manner, the following conduct is prohibited:

- Performing actions that may negatively affect Kandji or its users (e.g., Spam, Brute Force, Denial of Service, etc).
- Accessing, or attempting to access, data or information that does not belong to you.
- Delete, alter, share, retain, or destroy data or information that does not belong to you.
- Social engineering of any Kandji Personnel.
- Violating any laws or breaching any agreements in order to discover vulnerabilities.

Our Commitment to Researchers

If you responsibly report a vulnerability in accordance with this policy, we will:

- Within three (3) business days, we will promptly respond to and acknowledge the receipt of your report
- To the best of our ability, we will confirm the existence of your vulnerability to you and be as transparent as possible about what steps we are taking
- Provide an estimated timeframe for addressing the vulnerability
- Notify you when the vulnerability has been remediated.

All Vulnerabilities (The Default Policy)

Kandji will confidentially disclose discovered vulnerabilities to the organization that is in the best position to address that vulnerability with a resolution. That organization is the "responsible organization."

If the responsible organization is not a CVE Partner, Kandji will reserve a CVE ID.

In the interest of full transparency and to allow your organization sufficient time to address this issue, please be aware that Kandji follows the industry standard of a 90+30 disclosure deadline policy.

A vendor has 90 days after Kandji notifies them about a security vulnerability to make a patch available to users. If they make a patch available within 90 days, Kandji will publicly disclose details of the vulnerability 30 days after the patch has been made available to users.

If a vendor cannot patch an issue within the initial 90 days, Kandji will make the details of the vulnerability public at the end of the 90 days.

If the responsible organization is showing consistent good-faith effort to develop and ship an update, but cannot complete this work within 90 days, a 30-day extension may be granted at Kandji's sole discretion under the Default Policy (or for any of the enumerated exceptions below).

Grace Period

If a vendor cannot make a patch available in 90 days but will make a patch available within an additional 14 days (i.e., within 104 days since the vulnerability was disclosed to the vendor), Kandji may grant a grace period to the vendor upon request. In that case, Kandji will publicly disclose details of the vulnerability 120 days after the vulnerability was initially disclosed to the public.

Mutually-agreed early disclosure

In any of the above cases, Kandji and the relevant vendor can mutually agree to release details of a vulnerability earlier than the date indicated by policy.