Vulnerability Disclosure Policy

JUSFC is committed to protecting the public's information from unauthorized disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

Authorization

If we conclude your security research and vulnerability disclosure activities represent a good faith effort to comply with this policy, we will consider your research to be authorized and will not initiate or recommend any law enforcement or civil lawsuits related to such activities.

- You must comply with all applicable Federal, State, and local laws in connection with your security research activities.
- We do not authorize, permit, or otherwise allow (expressly or impliedly) any individual or entity to engage in any security research or vulnerability or threat disclosure activity that is inconsistent with this policy or the law. Those who engage in activities inconsistent with this policy or the law may be subject to criminal and/or civil liabilities.

We will work with you to understand and resolve the issue quickly and will not recommend or pursue legal action related to your research.

Should legal activity be initiated by a third party against you for authorized security research activities, we will take steps to make this authorization known.

Guidelines

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

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy incidents, 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. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to pivot to other systems.
- Provide us with 90 business days to resolve the issue before you disclose it publicly.
- Not submit a high volume of low-quality reports.

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

Unauthorized Test Methods

The following test methods are **NOT** authorized:

- Conducting network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g., office/facility or equipment access, open doors, tailgating)), or introducing any unauthorized device(s) on any JUSFC network (e.g., WiFi, computers, mobile devices, Bluetooth)
- Introducing malicious logic
- Testing any system or service other than the systems set forth in the Scope section.
- Conducting or engaging in social engineering (e.g., phishing, vishing) or any other non-technical vulnerability testing
- Altering, deleting, exfiltrating, sharing, or destroying JUSFC data

Scope

This policy applies only to the following public-facing JUSFC owned and controlled systems and services:

- JUSFC.gov
- Culcon.jusfc.gov

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing.

Vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any).

Although we develop and maintain other internet-accessible systems or services, we ask that *active research and testing* only be conducted on the systems and services covered by the scope of this policy.

If there is a system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

Reporting a Vulnerability

Vulnerability reports are accepted via email at jusfc[at]jusfc[dot]gov Acceptable formats are plain text, rich text, and HTML. We do not support PGP-encrypted emails.

Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 3 business days and will follow up with any actions we may take.

We do not provide payment for vulnerabilities reported, and by submitting a report to us, you waive any claims to compensation.

Information Use

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities.

If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely JUSFC, we may share your report with the Cybersecurity and Infrastructure Security Agency (CISA) where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without seeking your permission.

What to Include

In order to help us triage and prioritize submissions, we recommend that your reports:

- Offer a detailed summary that includes the issue(s), software product, versions, and configuration of software containing the vulnerability;
- Describe the location the vulnerability was discovered and the potential impact of exploitation;
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful);
- Be in English, if possible; and
- Include any scripts or exploit code in non-executable file types.

What You Can Expect from Us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 14 business days, we will acknowledge that your report has been received.
- We will attempt to confirm the existence of the vulnerability to you and be as transparent as possible about the steps we are taking during the remediation process, including on issues or challenges that may delay resolution.

Questions

Questions regarding this policy may be sent to jusfc[at]jusfc[dot]gov

Last updated March 5, 2021