Vulnerability Disclosure Policy
National Aeronautics and Space Administration
Office of the Chief Information Officer

December 3, 2024
Version 1.4

Introduction

The NASA Mission is to drive advances in science, technology, aeronautics, and space exploration to enhance knowledge, education, innovation, economic vitality and stewardship of the Earth. A great deal of NASA work leverages information technology to capture, interpret, and appropriately share scientific knowledge in the furtherance of its Missions and Programs. NASA is committed to protecting the confidentiality (where appropriate), integrity, and availability of its information and information systems.
NASA recognizes that external vulnerabilities can be discovered by anyone at any time and has issued this policy in order to provide clear guidelines to security researchers so that they feel comfortable reporting vulnerabilities they have discovered in good faith.
This vulnerability disclosure policy facilitates NASA's awareness of otherwise unknown vulnerabilities. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery and disclosure activities to help NASA meet its objectives, and to convey how to submit discovered vulnerabilities to NASA.

This policy describes

- What systems and types of research are covered under this policy
- General guidelines for demonstrating good faith
- How to submit vulnerability reports
- What to expect following a vulnerability report

Letters of Recognition (LOR)

• Not all submitted reports qualify for an LOR)
• Reports flagged as duplicates or identified as known issues do not qualify for an LOR.
• LORs are awarded exclusively for P1-P4 rated reports that have been validated, accepted, and confirmed as fixed.

Scope

Testing is only authorized on the targets listed as in scope. Any domain/property of The National Aeronautics and Space Administration not listed in the targets section is out of scope. Any service not expressly listed above, such as any connected services are excluded from scope and are not authorized for testing.
The following subsections define the systems and types of testing that are and are not in scope of this policy.

Systems

This policy applies to all NASA-managed systems that are accessible from the Internet. This includes the registered domain names:
• nasa.gov
• usgeo.gov
• scijinks.gov
• globe.gov

NASA internal-only services are not in scope and are not authorized for testing. Additionally, vulnerabilities found in non-federal systems from our vendors and contractors fall outside of this policy's scope and should be reported directly to the vendor or contractor according to their disclosure policy (if any).
Non-public NASA data is not authorized to reside on public third-party services. Although the third-party services themselves are not in scope, please report these data issues to NASA. The following types of non-public data are particularly sensitive, and warrant immediate reporting:

• Sensitive Personally Identifiable Information or PII (e.g., social security numbers);
• Financial information (e.g., credit card or bank account numbers);
• Proprietary information or trade secrets of companies of any party; and
• Documents with sensitivity markings (e.g., "Top Secret" or "ITAR/EAR").

Types of Testing

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

- Social engineering-based attacks (e.g., getting a user to click an attacker-controlled link).
- Denial of Service, Rate Limiting, or Spamming issues (e.g., layer 7 DOS attacks, Slowloris, etc.).
- Clickjacking on pages with no sensitive actions.
- Any reports with the endpoint /wp-json/wp/v2/users
- Any reports with the endpoint xmlrpc.php
- Attacks requiring physical access to a user's device
- Previously known vulnerable libraries without a working proof of concept.
- Content spoofing or text injection
- Reports from automated tools or scans without accompanying demonstration of exploitability
- Software version disclosure without accompanying demonstration of exploitability.
- Use of a known-vulnerable library without evidence of exploitability.
- Missing best practices. (Missing security headers, missing captcha, insecure certs)
- Insecure SSL or TLS issues (e.g., ciphers, certificates, etc.).
- Missing security headers (e.g., HTTP Strict-Transport-Security (HSTS), Content Security Policy (CSP), etc.) that do not lead directly to a vulnerability.
- Presence of the "autocomplete" attribute on web forms.
- Host header injections unless you can show how they can lead to stealing data
- Insecure cookie settings for non-sensitive cookies.
- Directory Listing
- Vulnerabilities affecting users of outdated browsers or platforms.
- Issues related to descriptive or verbose error messages.
- Any other non-technical vulnerability testing

Guidelines

NASA requests that security researchers make every effort to:

- Avoid impacting the availability of production systems.
- Notify NASA via the methods described in the policy as soon as possible after the discovery of a potential security issue.
- Keep all information about discovered vulnerabilities confidential until NASA approves the disclosure request.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction, modification, or exfiltration of NASA data.
- Only use exploits to the extent necessary to confirm the presence of a vulnerability. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or leverage the exploit to "pivot" to other systems.

• Once it is established that a vulnerability exists or any sensitive data is encountered (including personally identifiable information, financial information, proprietary information or trade secrets of any party), you must stop your test, NASA must be notified immediately, and details of the vulnerability or sensitive data shall not be disclosed to anyone else.
No compensation is available, other than NASA's gratitude for your help in advancing the NASA Mission. By submitting a vulnerability report, you waive all claims to compensation.

Authorization

If a security researcher makes a good faith effort to comply with this policy during security research, NASA will consider that research to be authorized, and will work with them to understand and resolve the issue quickly. In addition, NASA will not recommend or pursue legal action related to the research. Should legal action be initiated by a third party against a security researcher for activities that were conducted in accordance with this policy, NASA will make this authorization known.

Reporting a vulnerability

Bugcrowd is the official channel to report vulnerabilities for NASA systems, please refrain from submitting vulnerabilities via other avenues.

Submit reports via: https://www.bugcrowd.com/nasa-vdp

This reporting mechanism is not intended for use by NASA employees, contractors, and others with authorized IT access at NASA. NASA personnel should use NASA-internal IT support and reporting mechanisms rather than this program.
Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities.

We will acknowledge receipt of your report within three business days. Please keep your vulnerability reports current by sending us any new information as it becomes available. We may share your vulnerability reports with CISA, and any affected vendors or open source projects.

What NASA would like to see in a report

• In order to help us triage and prioritize submissions, NASA recommends that vulnerability reports:
• Describe the vulnerability, where it 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 the English language, if possible.
Please do not use this mechanism to report trivial system faults, such as typos or user interface errors not resulting in a vulnerability. NASA believes that public disclosure in the absence of a readily available mitigation will increase risk to NASA Missions. As a result, NASA requests that researchers refrain from sharing vulnerability reports with others for 90 days following the submission of the initial report, unless otherwise coordinated with NASA.

What a security researcher can expect from NASA

When a security researcher chooses to share their contact information with NASA, NASA is committed to coordinating a response with you as openly and as quickly as possible.

• Within three business days, NASA will acknowledge the receipt of a report.
• To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including issues or challenges that may delay resolution.
• We will maintain an open dialogue to discuss issues.

Safe Harbor

When conducting vulnerability research according to this policy, we consider this research to be:

• Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar state laws), and we will not initiate or support legal action against you for accidental, good faith violations of this policy;
• Exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for circumvention of technology controls;
• Exempt from restrictions in our Terms & Conditions that would interfere with conducting security research, and we waive those restrictions on a limited basis for work done under this policy; and
• Lawful, helpful to the overall security of the Internet, and conducted in good faith.
• You are expected, as always, to comply with all applicable laws.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please inquire via support@bugcrowd.com before going any further.