FEMA

Cyber Vulnerability Disclosure Policy for Public-Facing Systems and Services

FEMA Policy #404-21-001

BACKGROUND

Cybersecurity is strongest when the public is given the ability to contribute. A key component to receiving cybersecurity assistance from the public is to establish a formal policy that describes the actions that can be taken to identify and report vulnerabilities in a legally authorized manner. Such policies enable federal agencies to remediate vulnerabilities before they can be exploited by an adversary.

Vulnerabilities are often found in individual software components, in systems comprised of multiple components, or in the interactions between components and systems. They are typically exploited to weaken the security of a system, its data, or its users, with impact to their confidentiality, integrity, or availability. A primary purpose of remediating vulnerabilities is to protect people, in turn maintaining or enhancing their safety, security, and privacy.

An increasing number of organizations in the public and private sectors are adopting vulnerability disclosure policies to improve their ability to detect security issues on their networks that could lead to the compromise of sensitive data and the disruption of services.

PURPOSE

The Federal Emergency Management Agency (FEMA) is committed to protecting the public's information from unauthorized access or disclosure, and will work with members of the public who identify threats to our security. To facilitate those communications, FEMA created this policy to describe the manner in which information will be accepted about security vulnerabilities and how vulnerability reports may be disclosed to affected parties and/or the public. The content of this policy will be posted on a public webpage residing under FEMA's primary domain, FEMA.gov, and hyperlinks to that webpage will be placed on all public-facing systems and services within scope of the policy. This policy does not supersede or modify any existing FEMA policy.

The goal of this cyber vulnerability disclosure policy is to ensure a broad, shared understanding of the overlapping interests between security researchers and FEMA

with respect to systems or services discovered to be vulnerable, to adopt a consensus on principles and practices to promote better collaboration, and to frame a consistent and reliable practice for the disclosure and remediation process.

This policy is intended to provide security researchers with clear guidance for conducting vulnerability discovery activities and submitting information on discovered vulnerabilities to FEMA. The policy applies to all members of the general public, which also includes all federal employees and contractors.

This policy describes what systems and types of research are covered, how to send FEMA vulnerability reports, and how long FEMA will ask security researchers to wait before publicly disclosing vulnerabilities.

Anyone conducting security research in accordance with this policy will be called a "researcher," and anyone reporting a discovered security vulnerability to FEMA in accordance with this policy will be called a "reporter" in this policy.

PRINCIPLES

The following principles and/or values will guide the implementation of the policy.

A. FEMA is committed to protecting the security and privacy of its data, systems, and the public. Governments maintain legitimacy by keeping the trust of their citizens, and a security flaw found on a .gov host can erode that confidence. When government systems are exposed by weak configuration or technical vulnerability, the security of the information, the privacy of its citizen-owners, and the reputation of its custodians are at risk.

B. FEMA is committed to protecting the trust involved in the process of identifying, addressing, and remediating security vulnerabilities. Information sharing is only effective when the participants trust each other and share their expectations of privacy, data use, and future communications.

REQUIREMENTS

A. Published Conditions

Outcome: Anyone wishing to communicate to FEMA about a discovered or potential security vulnerability understands the criteria for authorized and unauthorized activity.

1. FEMA will work with the reporter to understand and resolve the issue quickly.

FEMA

2. Authorized Security Vulnerability Research

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

   a. Notify FEMA as soon as possible after discovering a real or potential security issue;
   b. Make every effort to avoid privacy incidents, degradation of user experience, disruption to production systems, and destruction or manipulation of data;
   c. Only use exploits to the extent necessary to confirm a vulnerability;
   d. Provide FEMA with 90 business days to resolve the issue before disclosing it publicly; and
   e. Avoid submitting a high volume of low-quality reports.

3. Once it has been established that a vulnerability does exist or that any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party) has been encountered, the researcher must stop the testing, immediately notify the FEMA Vulnerability Disclosure Team at FEMA-VDP@fema.dhs.gov, and not disclose the vulnerability or data to anyone else.

4. The following test methods are **not** authorized:
   a. Conducting network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data;
   b. Physical testing (e.g., gaining physical access to any FEMA office/facility or equipment through open doors, tailgating, etc.), or introducing any unauthorized device(s) on any FEMA network (e.g., Wi-Fi routers, computers, mobile devices, Bluetooth devices);
   c. Introducing malicious logic;
   d. Testing of any system or service other than those set forth in the Scope section of this policy;
   e. Conducting or engaging in social engineering to obtain information from any FEMA personnel (e.g., phishing, vishing), or any other non-technical vulnerability testing; and
   f. Altering, deleting, exfiltrating, sharing, or destroying any data contained in FEMA systems under any circumstance.

5. Scope
   a. This policy applies to the following public-facing FEMA-owned and controlled systems and services, identified by domain and/or URL:

      - FEMA.gov
      - DisasterAssistance.gov
      - FirstResponderTraining.gov
      - Floodsmart.gov

- Listo.gov
- Ready.gov
- ReadyBusiness.gov

b. Any services not falling within the scope above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from FEMA's vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any).

c. If there is any question about whether a system or service is within scope or not, the FEMA Vulnerability Disclosure Team (or the security contact for the system's domain name as listed in the .gov WHOIS) should be contacted before starting the research.

d. Though FEMA may develop and maintain internet-accessible systems or services other than those listed on the public webpage, *active research and testing* is only authorized to be conducted on the systems and services covered by the scope of this policy.

e. If there is a system not in scope that the researcher thinks merits testing, the FEMA Vulnerability Disclosure Team must be contacted at FEMA-VDP@fema.dhs.gov to discuss it prior to any testing.

f. This scope will be increased over time.

B. REPORTING A VULNERABILITY

Outcome: Security researchers have the necessary tools, guidance, and opportunity to report any discovered or potential security vulnerability to FEMA and expect consistent and reliable processing of the submission.

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

   a. If the reporter's findings include newly discovered vulnerabilities that affect all users of a product or service and not solely FEMA, FEMA's Vulnerability Disclosure Team may share the report with the Cybersecurity and Infrastructure Security Agency (CISA), where it will be handled under its coordinated vulnerability disclosure process.[1]

   b. FEMA will not share the reporter's name or contact information without seeking the reporter's express permission.

[1] CISA Coordinated Vulnerability Disclosure (CVD) Process, https://www.cisa.gov/coordinated-vulnerability-disclosure-process.

2. FEMA does not provide payment for vulnerabilities reported, and by submitting a report to FEMA, the researcher waives any claims to compensation.

3. Submission Format
   a. FEMA will accept vulnerability reports via email at FEMA-VDP@fema.dhs.gov. Acceptable formats will be plain text, rich text, and HTML.
   b. FEMA will accept reports that are submitted anonymously. If contact information is shared, FEMA's Vulnerability Disclosure Team will acknowledge receipt of the report within three (3) business days.
   c. FEMA does not support PGP-encrypted emails.

4. Requested Information (i.e., what FEMA would like from the reporter):
   a. In order to help FEMA triage and prioritize submissions, the reports should include, at a minimum:
      i. A detailed summary that includes the issue(s), software product, versions, and configuration of software containing the vulnerability;
      ii. A description of the location where the vulnerability was discovered and the potential impact of exploitation;
      iii. A detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful);
      iv. All information in English, if possible; and
      v. Any scripts or exploit code in non-executable file types.

5. What the reporter can expect from FEMA:
   a. FEMA is committed to coordinating as openly and quickly as possible with reporters who choose to share their contact information.
   b. Within three (3) business days, FEMA will acknowledge receipt of the report.
   c. FEMA will attempt to confirm the existence of the vulnerability to the reporter and be as transparent as possible about steps that are being taken during the remediation process, including on issues or challenges that may delay resolution.

C. LEGAL

1. The reporter must comply with all applicable federal, state, and local laws in connection with the security research activities.

2. FEMA does 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.

3. If FEMA concludes the security research and vulnerability disclosure activities represent a good faith effort to follow the restrictions and guidelines set forth in this policy, FEMA will determine that the security research has been authorized and will not initiate or recommend any law enforcement or civil lawsuits related to such activities.

4. In the event that a third party initiates legal activity against the reporter for authorized security research activities, FEMA will take steps to make it known that the reporter's activities were conducted pursuant to and in compliance with this policy.

LYTWAIVE L HUTCHINSON

Digitally signed by LYTWAIVE L HUTCHINSON
Date: 2021.05.05 08:48:47 -04'00'

Lytwaive L. Hutchinson
FEMA Chief Information Officer

FEMA

ADDITIONAL INFORMATION

REVIEW CYCLE

FP 404-21-001, "Cyber Vulnerability Disclosure Policy for Public-Facing Systems and Services" will be reviewed, reissued, revised, and/or rescinded within four (4) years of the issue date.

AUTHORITIES AND REFERENCES

Authorities

A. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), Binding Operational Directive 20-01, "Develop and Publish a Vulnerability Disclosure Policy"
B. Office of Management and Budget (OMB) Memorandum M-20-32, "Improving Vulnerability Identification, Management, and Remediation"
C. 44 U.S.C. §§ 3552-3554, "Information Security"

Note: Policies do not have the force and effect of law, except as authorized by law or as incorporated into a contract.

References

A. CISA Coordinated Vulnerability Disclosure (CVD) Process
B. The CERT® Guide to Coordinated Vulnerability Disclosure
C. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 29147:2018, "Information Technology - Security Techniques - Vulnerability Disclosure"
D. ISO/IEC 30111:2019, "Information Technology — Security Techniques — Vulnerability Handling Processes"
E. NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations"

DEFINITIONS

Service: An information technology (IT) service is provided to one or more customers, by an IT service provider. An IT service is based on the use of IT and supports the agency's business process. An IT service consists of a combination of people, processes, and technology. Sometimes IT systems are acquired as tools for users, but most of the time, a government IT system is the backend implementation of an information service.

Social Engineering: The use of deception to manipulate individuals into divulging confidential or personal information or to act contrary to security protocols.

System: An IT system is an underlying automated technological component used to provide an IT service or services to users or other information systems/applications. In some cases, a service and system may have the same name, but most IT systems exist to deliver information or implement a service. A "system" is often simply a tool that exists to make some task easier or possible, typically utilizing Web technologies. By itself, the operation of an IT system could be a service, but it is the mission function that the system enables that is the actual service being provided.

Triage: Initial post-detection response to a suspected incident.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Such a weakness can be used by a party to cause the software to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness. Vulnerabilities are often found in individual software components, in systems comprised of multiple components, or in the interactions between components and systems. They are typically exploited to weaken the security of a system, its data, or its users, with impact to their confidentiality, integrity, or availability.

Vulnerability Disclosure: The act of initially providing vulnerability information to a party that was not believed to be previously aware. The individual or organization that performs this act is called the "reporter."

MONITORING AND EVALUATION

The Office of the Chief Information Officer will monitor implementation of this policy and completion of relevant guidance to support this policy. Lessons learned, questions, and concerns raised related to the implementation of this policy will be used to inform future revisions.

QUESTIONS

Address any questions or concerns, or report potential or discovered vulnerabilities in FEMA systems and/or services, to the FEMA Vulnerability Disclosure Team at FEMA-VDP@fema.dhs.gov.