Department of Energy
Southwestern Power Administration
One West Third Street
Tulsa, Oklahoma 74103-3502

Vulnerability Disclosure Policy

Southwestern Power Administration
03/01/2021

Introduction

Southwestern Power Administration (Southwestern) is committed to ensuring the security of the American public by protecting the public's information. The Vulnerability Disclosure Policy (VDP) is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey Southwestern's preferences in how to submit discovered vulnerabilities.

Southwestern's VDP describes: (1) what systems and types of research are covered; (2) how to send Southwestern vulnerability reports; (3) and how long Southwestern asks security researchers to wait before publicly disclosing vulnerabilities.

Southwestern encourages researchers to contact us to report potential vulnerabilities in our systems.

Authorization

Good faith efforts to comply with the VDP during security research will be considered to be authorized. In the context of the VDP, "good faith" means security research conducted with the intent to follow the VDP without malicious motive. Southwestern may evaluate a researcher's intent on multiple bases, including by the researcher's actions, statements, and the results of the researcher's actions.

Good faith security research is considered to be accessing a computer or software solely for purpose of testing or investigating a security flaw or vulnerability and disclosing those findings in alignment with the VDP. A researcher's actions should be consistent with an attempt to improve security and to avoid doing harm, either by unwarranted invasions of privacy or causing damage to property.

Southwestern will work with researchers to understand and resolve issues identified during the course of researcher's good faith efforts and will not recommend or pursue legal action related to the research. Should legal action be initiated by a third party against a researcher for activities that were conducted in accordance with this VDP, Southwestern will make this authorization known.

Guidelines

Under this VDP, "research" means activities in which the researcher:

- Notifies Southwestern as soon as possible after a real or potential security issue is discovered.
- Makes every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only uses exploits to the extent necessary to confirm a vulnerability's presence and does not use an exploit to compromise or exfiltrate data, establish persistent command line access, or pivot to other systems.
- Provides Southwestern a reasonable amount of time to resolve issues before disclosing them publicly.
- Does not submit a high volume of low-quality reports.

Once a researcher has established that a vulnerability exists or encounters any sensitive data (including personally identifiable information, financial information, or proprietary information/trade secrets of any party), **the researcher must stop their test, notify Southwestern immediately, and refrain from disclosing the discovered data to any other party**.

Test methods

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

- 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 access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing.

Before the start of any testing, the researcher should provide the following information to the Southwestern VDP team at VDP@swpa.gov:

- Dates/Times of testing
- The IP address(es) that will be used for testing.
- What assets will be tested (see scope below)

Providing this information beforehand will ensure any benign testing is not treated as a cyber security incident by Southwestern.

Scope

This policy applies to the following systems and services:

- www.swpa.gov
- swpa.gov services, including the following hostnames:
    - svpn.swpa.gov
    - tvpn.swpa.gov
    - nvpn.swpa.gov
    - titan.swpa.gov
    - hyperion.swpa.gov

Any service not expressly listed above, such as any connected services, are excluded from scope and ARE NOT AUTHORIZED for testing. Additionally, vulnerabilities found in systems from Southwestern's vendors fall outside of the scope of this VDP and should be reported directly to the vendor according to the vendor's disclosure policy (if applicable). If a researcher is unsure whether a system is in scope, the researcher should contact Southwestern's VDP team at VDP@swpa.gov before starting the research.

Though Southwestern develops and maintains 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 VDP. If there is a particular system not in scope that a researcher thinks merits testing, please contact Southwestern to discuss it first. Southwestern reserves the right to increase or decrease the scope of this VDP at any time.

Reporting a vulnerability

Information submitted under this VDP will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If a researcher's findings include newly discovered vulnerabilities that affect all users of a product or service and not solely Southwestern, we may share your report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. Southwestern will not share your name or contact information without express permission.

Southwestern accepts vulnerability reports via VDP@swpa.gov. Reports may be submitted anonymously. If a researcher shares contact information, Southwestern will acknowledge receipt of the researcher's report within 3 business days. **By submitting a vulnerability, a researcher acknowledges that he or she has no expectation of payment and that the researcher expressly waives any future pay claims against the U.S. Government related to the researcher's submission.**

Southwestern does not support PGP-encrypted emails.

Southwestern's Expectations

To help Southwestern triage and prioritize submissions, Southwestern recommends that a researcher's report:

- Describe the location where 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 written in English, if possible.

Researcher's Expectations

When a researcher chooses to share his or her contact information with Southwestern, we commit to coordinating with the researcher as openly and as quickly as possible.

- Within 3 business days, Southwestern will acknowledge that the researcher's report has been received.
- To the best of Southwestern's ability, we will confirm the existence of the vulnerability to the researcher and be as transparent as possible about what steps we are taking during the remediation process, including communication of issues or challenges that may delay resolution.
- Southwestern will maintain an open dialogue to discuss issues.

Questions

Questions regarding this VDP may be sent to the Southwestern VDP team at VDP@swpa.gov. Southwestern also invites researchers to contact us with suggestions for improving this VDP.

Document Change History

Version	Date	Description
1.0	03/01/2021	First issuance.