PJM Vulnerability Disclosure Policy

Purpose

This program is intended to give security researchers terms and conditions for conducting vulnerability discovery activities directed at publicly accessible PJM Interconnection (PJM) information systems and submitting discovered vulnerabilities to PJM. If questions arise, please take no action until that action is discussed with the VDP lead at PJM.

Introduction

Maintaining the security of our networks and system is a high priority at PJM. Our information technologies provide critical services for the safety, reliability and security of the bulk power system. 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.

This policy describes **what systems and types of research** are covered under this policy, **how to send us** vulnerability reports, and **how long** PJM asks security researchers to wait before publicly disclosing vulnerabilities.

We encourage you to contact us at the address listed below to report potential vulnerabilities in our systems.

Authorization

If you engage in Good Faith Security Research (as defined below) and make a good faith effort to comply with this policy during your security research, PJM will consider your research to be authorized under the Computer Fraud and Abuse Act and related laws. We will work with you to understand and resolve the issue quickly, and PJM will not recommend or pursue legal action related to your research.

Guidelines

Under this policy, “Good Faith Security Research” means activities in which you:

- Access a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability.
- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations or other harm to individuals or the public, 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 intentionally access or exfiltrate data, establish persistent command line access, or pivot to other systems.

- Provide us 180 days' time to resolve the issue before you disclose it publicly or to any other party.
- Do not submit a high volume of low-quality reports.
- Do not threaten or try to extort PJM.

Test Methods

The following test methods are NOT authorized:

- Testing on systems or networks not managed by PJM (i.e. PJM members)
- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Brute-force attacks
- Targeting PJM employees or its customers, including through social engineering attacks or phishing attacks
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing
- Social engineering, including sending phishing messages
- Introducing malicious software
- Methods that disrupt system operation or result in the modification or destruction of data
-

Exploitation of a vulnerability beyond the minimal amount of testing required to prove a vulnerability exists or to identify an indicator related to a vulnerability

Scope

Publicly accessible information systems, web property, or data owned, operated, or controlled by PJM including the following domains:

- WWW.PJM.COM
- DATAVIEWER.PJM.COM
- DATAMINER2.PJM.COM
- ACCOUNTMANAGER.PJM.COM
- BBOARD.PJM.COM
- GASPIPE.PJM.COM
- POWERMETER.PJM.COM
- CAPACITYEXCHANGE.PJM.COM

How to Submit a Report

Please provide a detailed summary of the vulnerability, including: type of issue; product, version, and configuration of software containing the bug; step-by-step instructions to reproduce the issue; proof-of-concept; impact of the issue; and suggested mitigation or remediation actions, as appropriate. The report should be provided via email to: securityVDP@Pjm.com.

By submitting a vulnerability report to this address, you are indicating that you have read, understand, and agree to the terms and conditions of the program for the conduct of security research and disclosure of vulnerabilities or indicators of vulnerabilities related to publicly accessible PJM information systems.

What You Can Expect From Us

We take every disclosure seriously. We will investigate every disclosure and strive to ensure that appropriate steps are taken to mitigate risk and remediate all reported vulnerabilities.

PJM remains committed to coordinating with the security researcher transparently and promptly. This includes taking the following actions:

- Within five business day, PJM will acknowledge receipt of your report. PJM's security team will investigate the report and may contact you for further information.
- When practicable and authorized, PJM will confirm the existence of the vulnerability to the researcher and keep the researcher informed, as appropriate, while remediation of the vulnerability is under way.
- PJM wants researchers to be recognized publicly for their contributions, if that is the researcher's desire. However, public disclosure of vulnerabilities will only be authorized at the expiration of the 180 day resolution period.

Legal

This policy does not grant authorization, permission, or otherwise allow express or implied access to PJM information systems , intellectual property, trademark to any individual, group of individuals, consortium, partnership, or any other business or legal entity.

PJM may modify the terms and conditions or terminate the program at any time.

Document Change History

Version	Date	Description
Version 1.0	April 22, 2024	Initial release to PJM.COM