Vulnerability Disclosure Policy

At WPS, we work hard to protect all data within our systems, applications, platforms, and services. We appreciate all well-intentioned persons who seek to help us in our mission to continually improve our security practices by conducting security research on our public-facing websites and applications and reporting all findings to WPS Information Security. All security research activities are subject to the WPS Vulnerability Disclosure Policy. This policy includes instructions for submitting vulnerabilities to WPS. You must abide by this policy at all times when conducting security research and reporting potential vulnerabilities in WPS public-facing websites and applications.

Introduction

WPS is committed to ensuring the security of our customers and partners by protecting their information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and reporting the same to WPS.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and restrictions on public disclosure of vulnerabilities.

We encourage security researchers to report vulnerabilities they've discovered as set out in this policy.

Authorization

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

Guidelines

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

- Notify WPS as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Should a privacy violation, degradation of user experience, disruption to production systems, or destruction or manipulation of data occur during testing, you agree to cease testing immediately and notify WPS.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. 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 WPS a reasonable amount of time (typically 90 days) to resolve the issue before you disclose it publicly.
- You do not intentionally compromise the privacy or safety of WPS personnel, customers, or any third parties.
- You do not intentionally compromise the intellectual property or other commercial or financial interests of any WPS personnel or entities, customers, or any third parties.

Once you've established that a vulnerability exists or 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 WPS immediately, and not disclose this data to anyone else.**

Scope

All systems and services associated with WPS domains are in scope. Subdomains are considered within scope, if their parent domains are within scope. Additionally, any website published with a link to this policy shall be considered in scope. Vulnerabilities found in non-WPS 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). If you aren't sure whether a system or endpoint is in scope or not, contact security@wpsic.com before starting your research.

Rules of Engagement

Security researchers must not:

- Engage in physical testing of facilities or resources
- Engage in social engineering
- Send unsolicited electronic mail to WPS users, including "phishing" messages
- Execute or attempt to execute "Denial of Service" or "Resource Exhaustion" attacks
- Introduce malicious software
- Test in a manner which could degrade the operation of WPS systems; or intentionally impair, disrupt, or disable WPS systems
- Test third-party applications, websites, or services that integrate with or link to or from WPS systems
- Delete, alter, share, retain, or destroy WPS data, or render WPS data inaccessible
- Use an exploit to exfiltrate data, establish command line access, establish a persistent presence on WPS systems, or "pivot" to other WPS systems
- Disclose vulnerability information in a way other than as allowed herein

WPS™
A HEALTH SOLUTIONS COMPANY

Security researchers may:

- View or store WPS nonpublic data only to the extent necessary to document the presence of a potential vulnerability

Security researchers must:

- Cease testing and notify us immediately upon discovery of a vulnerability
- Cease testing and notify us immediately upon discovery of an exposure of nonpublic data
- Purge any stored WPS nonpublic data upon reporting a vulnerability
- Disclose vulnerability information as set forth in the 'Reporting a Vulnerability' and 'Disclosure' sections below

Reporting a Vulnerability

We accept vulnerability reports at security@wpsic.com. Reports may be submitted anonymously and will hold your information confidence if requested. **Please include any information obtained regarding the vulnerability including:**

- A description of the vulnerability,
- Location of the vulnerability,
- Validation steps taken to confirm the vulnerability,
- Any impact to nonpublic data or adverse impacts to WPS systems and information which occurred during testing, and
- Potential impact of the vulnerability being exploited.

Information submitted under this policy will be used for defensive purposes only—to mitigate or remediate vulnerabilities. We will not share your name or contact information without express permission.

By conducting security research on WPS systems, you are indicating that you have read, understand, and agree to the guidelines described in this policy for the conduct of security research and disclosure of vulnerabilities or indicators of vulnerabilities related to WPS information systems. Further, by submitting a vulnerability disclosure to WPS, you consent to having the contents of the communication and follow-up communications stored on WPS systems.

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

- Adhere to all legal terms and conditions outlined herein
- 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)

Disclosure

WPS is committed to timely correction of vulnerabilities. However, we recognize that public disclosure of a vulnerability in absence of a readily available corrective action likely increases versus decreases risk. Accordingly, we require that you refrain from sharing information about discovered vulnerabilities for 90 calendar days after you have received our acknowledgement of receipt of your report. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, we require that you coordinate in advance with WPS via email at security@wpsic.com.

We may share vulnerability reports with any affected vendors or third parties. We will not share names or contact data of security researchers unless given explicit permission.

Questions

Questions regarding this policy may be sent to security@wpsic.com. We also invite you to contact us with suggestions for improving this policy.

WPS™
A HEALTH SOLUTIONS COMPANY