WIDEPOINT

ALL PROGRAMS

PUBLIC VULNERABILITY DISCLOSURE POLICY

[WP-NC-VulDisc-Pol]

Version 1.0

April 11, 2023

11250 Waples Mill Road
South Tower, Suite 210
Fairfax, VA 22030

Notice: Operational Research Consultants, Inc. (ORC), a wholly-owned subsidiary of WidePoint Corporation, has changed its legal name to WidePoint Cybersecurity Solutions Corporation, hereafter referred to simply as WidePoint. This is a legal name change only for branding purposes with no change to ownership, corporation type or other status. Any and all references to "WidePoint" within this document refers specifically and only to WidePoint Cybersecurity Solutions Corporation, the wholly-owned subsidiary of WidePoint Corporation, and not to WidePoint Corporation as a whole.

© Copyright 2023, WidePoint Cybersecurity Solutions Corporation
All Rights Reserved

Document Signature Page

Godfrey.Caroline.R.
ORC3011044657.ID

Digitally signed by
Godfrey.Caroline.R.ORC3011044657.
ID
Date: 2023.04.11 15:02:53 -04'00'

Caroline Godfrey, WidePoint Chief Security Officer

Webb.Richard.David.ORC
2990000230.ID

C=US, O=U.S. Government, OU=ECA,
OU=ORC, OU=WidePoint Cybersecurity,
CN=Webb.Richard.David.ORC29900002
30.ID
Reviewed WidePoint Public
Vulnerability Disclosure Policy
2023-04-11 13:55:17

Richard Webb, WidePoint Corporate Security Auditor

Brown.Benjamin.J.ORC3011028990.ID

Brown.Benjamin.J.ORC3011028990.ID
C=US, O=U.S. Government, OU=ECA, OU=
ORC, OU=WidePoint Cybersecurity
Solutions Corporation, CN=
Brown.Benjamin.J.ORC3011028990.ID
I am approving this document
2023.04.11 14:49:16-04'00'

WidePoint Lead Certificate Authority Administrator

Weinberg.Micha
el.J.ORC301100
3708.ID

Digitally signed by
Weinberg.Michael.J.ORC3011003708.ID
DN: C=US, O=U.S. Government, OU=ECA,
OU=ORC, OU=WidePoint Cybersecurity
Solutions Corporation, CN=
Weinberg.Michael.J.ORC3011003708.ID
Reason: I am approving this document
Date: 2023.04.11 15:25:35-04'00'

WidePoint Lead System Administrator

© Copyright 2023, WidePoint Cybersecurity Solutions Corporation
All Rights Reserved

DOCUMENT REVISION HISTORY

Date	Version	Description of Change	Author
2023-03-17	1.0	Initial version	Richard Webb

© Copyright 2023, WidePoint Cybersecurity Solutions Corporation
All Rights Reserved

TABLE OF CONTENTS

© Copyright 2023, WidePoint Cybersecurity Solutions Corporation
All Rights Reserved

1 WIDEPOINT PUBLIC VULNERABILITY DISCLOSURE POLICY

This WidePoint Public Vulnerability Disclosure Policy is a requirement under the WidePoint System Security Plan, in particular, the Risk Assessment Control Family Control RA-5(11) Vulnerability Scanning and Monitoring | Public Disclosure Program. This policy has been modeled on the Vulnerability Disclosure Policy of the Department of Justice (found here: https://www.justice.gov/jmd/vulnerability-disclosure-policy) and does not intend any authority derived from the Department of Justice or any other department, agency, or entity other than WidePoint.

1.1 PURPOSE

WidePoint is committed to ensuring the security and the privacy of WidePoint applicants and subscribers by safeguarding their digital information. This WidePoint Public Vulnerability Disclosure Policy provides guidelines for the cybersecurity research community and members of the general public (hereafter referred to as researchers) on conducting good faith vulnerability discovery activities directed at public facing WidePoint websites and services. This WidePoint Vulnerability Disclosure Policy also instructs researchers on how to submit discovered vulnerabilities to the WidePoint Chief Security Officer and the WidePoint Management Team.

1.2 AUTHORIZED ACTIVITIES

If a researcher complies with this policy in conducting vulnerability discovery activities, WidePoint will consider those activities to be authorized.

1.3 OVERVIEW

WidePoint issues digital certificates and credentials to customers and services that have a need to interface securely with a government entity, a business, or other individuals and services. As part of this digital certificate and credential issuance process, personal data is gathered as WidePoint performs a verification of the identity documentation provided by the applicant, subscriber or service (by the human that is sponsoring that service) that is requesting a digital certificate or credential in accordance with NIST SP 800-63 Digital Identity Guidelines at varying levels of assurance. A level of assurance is a measure of the certainty that the applicant, subscriber, or service presenting identity verification documentation for a WidePoint digital certificate or credential is who they say they are. Higher levels of assurance require more identity verification of documentation or the capturing of biometrics from the applicant or subscriber. This information is gathered in both written and electronic forms and is stored in the secure systems operated by WidePoint in order to manage the life-cycle of the digital certificate or credential issued to the applicant, subscriber or service. WidePoint digital certificates and credentials provide government agencies, businesses, applications, networks and services assurance that the person or service that is authenticating to their systems is who/what they say they are.

WidePoint recognizes that the cybersecurity research community regularly makes valuable contributions to the cybersecurity of individual organizations and the broader Internet. WidePoint recognizes that fostering a positive relationship with this community can help improve the security of WidePoint and its customers.

Vulnerabilities submitted to WidePoint under this policy will be used for defensive purposes – to mitigate or remediate vulnerabilities in our networks and services, or those of our vendors.

Researchers must review, understand, and abide by the following terms and conditions before conducting any research or testing on WidePoint networks or applications and before submitting a report.

© Copyright 2023, WidePoint Cybersecurity Solutions Corporation
All Rights Reserved

1.4 General Guidelines

As described in more detail below, to be considered authorized activities under this policy, researchers must:

- Notify WidePoint within 72 hours of discovering any real or potential security vulnerabilities.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only conduct testing activities to the extent necessary to confirm a vulnerability's presence.
- Not use any exploit to compromise or exfiltrate data; open, take, or delete files; establish command line access and/or persistence; or pivot to other systems.
- Not escalate privileges or attempt to move laterally within the network.
- Not disrupt access to WidePoint services or introduce any malware in the course of testing.
- Not publicly disclose reported vulnerabilities without prior coordination with WidePoint.
- Not submit a high volume of low-quality reports.

Once a researcher establishes that a vulnerability exists, or encounters any sensitive data (including personally identifiable information, financial information, or the proprietary information or trade secrets of any party), they must stop testing, notify WidePoint immediately through our vulnerability submission process as described in Section 1.7 Reporting a Vulnerability, and not disclose this data to anyone else.

1.5 Test Methods

WidePoint will deal in good faith with researchers who discover, test, and submit vulnerabilities or indicators of vulnerabilities in accordance with the following guidelines:

- Testing activities are limited exclusively to
  - (1) Testing to detect a vulnerability or identify an indicator related to a vulnerability; or
  - (2) Sharing information with, or receiving information from, WidePoint about a vulnerability or an indicator related to a vulnerability.
- Researchers may not harm any WidePoint system or data on a WidePoint system or exploit any potential vulnerabilities beyond the minimal amount of testing required to prove that a vulnerability exists or to identify an indicator related to a vulnerability.
- Researchers must not establish command line access and/or persistence; pivot to other systems; escalate privileges; attempt to move laterally within the network; disrupt access to WidePoint services; or introduce any malware in the course of testing.
- Researchers must avoid intentionally accessing the content of any communications, data, or information transiting or stored on any WidePoint information system – except to the extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.
- Researchers must not intentionally exfiltrate or copy WidePoint data, or open, take, or delete files. Should researchers obtain WidePoint data during their research, they must coordinate with WidePoint to ensure that data is appropriately destroyed upon confirmation that the vulnerability is remediated.
- Researchers may not intentionally compromise the privacy or safety of WidePoint personnel (e.g., employees, contractors, or parties to ongoing investigations) or any third parties.
- Researchers may not intentionally compromise the intellectual property or other commercial or financial interests of any WidePoint personnel or entities or any third parties through their research.
- Researchers may not publicly disclose any details of the vulnerability, indicator of vulnerability, or the content of information rendered available by a vulnerability, until that vulnerability is remediated and they receive explicit written authorization from WidePoint.

© Copyright 2023, WidePoint Cybersecurity Solutions Corporation
All Rights Reserved

- Researchers may not conduct denial-of-service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Researchers may not conduct physical testing or social engineering, including spear phishing, of WidePoint personnel or contractors.
- Researchers may not intentionally submit a high-volume of low-quality, unsubstantiated, or false-positive reports.

If at any point researchers are uncertain whether to continue testing, researchers must engage with WidePoint at the email address provided below before conducting any further testing.

1.6 Scope of Policy

Any services not explicitly identified here are considered out-of-scope and are not authorized for testing. The scope of WidePoint assets subject to this policy will be updated regularly. If a researcher is unsure whether a system is in scope or not, contact WidePoint at Vulnerability-Disclosure AT Widepoint DOT com before starting any testing (or at the security contact for the system's domain name listed in the .gov WHOIS).

The following domains are in-scope for testing:

- www.widepoint.com
- www.orc.com
- orc.widepoint.com
- eca.orc.com
- ssp.orc.com
- nfi.orc.com
- eva.orc.com
- ssp.eva.orc.com
- nfi.eva.orc.com

1.7 Reporting a Vulnerability

If a vulnerability is discovered, researchers must provide a detailed summary of the vulnerability, including the following:

- description of the vulnerability and its potential impact;
- product, version, and configuration of any software or hardware potentially impacted;
- step-by-step instructions to reproduce the issue;
- proof-of-concept; and
- suggested mitigation or remediation actions, as appropriate.

WidePoint will accept vulnerability disclosure reports through by email at Vulnerability-Disclosure AT Widepoint DOT com. When submitting sensitive material, WidePoint recommends encrypting the data.

By submitting a report, WidePoint will presume that the submitter read, understands, and agrees to the guidelines described in this policy, and consents to having any subsequent communications with WidePoint stored on a WidePoint information system. Personal data submitted in a vulnerability disclosure report will not be retained by WidePoint, other than contact information that will only be retained in order to coordinate with the researcher.

If a researcher discovers a zero-day or any new vulnerability that may affect all users of a product or service and not solely WidePoint, WidePoint may share a vulnerability disclosure report with the Cybersecurity and

© Copyright 2023, WidePoint Cybersecurity Solutions Corporation
All Rights Reserved

Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without your express permission.

1.8 What You Can Expect From WidePoint

WidePoint will take every disclosure report seriously and, to the extent it deems appropriate, investigate every report to validate the vulnerability, prioritize the risk, and ensure that appropriate steps are taken to mitigate risk and remediate reported vulnerabilities.

WidePoint remains committed to coordinating with the security research community as openly and quickly as possible. This includes:

- ➢ Acknowledging receipt of each vulnerability report within three (3) business days. WidePoint's security team or its partners will investigate each report, and may contact the researcher for further information.
- ➢ Confirming the existence of the vulnerability to the researcher to the best of our ability and informing the researcher of any issues or challenges that may delay resolution. If necessary, WidePoint or its partners may coordinate with the researcher for additional information as we work to remediate a vulnerability.
- ➢ Maintaining an open dialogue with individual researchers to discuss issues.
- ➢ If researchers conduct vulnerability disclosure activities in accordance with the restrictions and guidelines set forth in this policy, (1) WidePoint will not initiate or recommend any law enforcement or civil actions related to such activities, and (2) in the event of any law enforcement or civil action brought in connection with research activities, WidePoint will take steps to make known that your activities were conducted pursuant to and in compliance with this policy.

1.9 Activities Outside the Scope of This Policy

WidePoint does not authorize, permit, or otherwise allow (expressly or impliedly) any person, including any individual, group of individuals, consortium, partnership, or any other business or legal entity, to engage in any security research or vulnerability or threat disclosure activity on or affecting WidePoint systems that is inconsistent with this policy or the law. If you engage in any activities that are inconsistent with this policy or other applicable law, you may be subject to criminal and/or civil liabilities.

To the extent that any security research or vulnerability disclosure activity involves the networks, systems, information, applications, products, or services of a non-WidePoint entity (e.g., other Federal departments or agencies; State, local, or Tribal governments; private sector companies or persons; employees or personnel of any such entities; or any other such third party), those third parties may independently determine whether to pursue legal action or remedies related to such activities.

This policy does not in any way limit the authority of WidePoint to pursue legal action. Nor will actions taken in accordance with this policy shield an individual from prosecution for any previous or future violations of the law.

1.10 Modification or Termination of This Policy

WidePoint may modify the terms of this policy or terminate the policy at any time.

1.11 Questions

Questions regarding this policy may be sent to Vulnerability-Disclosure AT Widepoint DOT com. We also invite you to contact us with suggestions for improving this policy.

© Copyright 2023, WidePoint Cybersecurity Solutions Corporation
All Rights Reserved