Vulnerability Disclosure Program

Contents

Introduction

At Ivanti, we are dedicated to ensuring the security and integrity of our enterprise software products. We recognize the vital role that security researchers, ethical hackers, and the broader security community play in identifying and reporting vulnerabilities. This Vulnerability Disclosure Policy outlines our commitment to working collaboratively with security researchers to improve the security of our software. It outlines steps for reporting vulnerabilities, what we expect, and what you can expect from us.

If you encounter any security-related issues involving Ivanti Products or Solutions, including those related to products from companies acquired by Ivanti (such as Pulse Secure, Cherwell and MobileIron), or if you have security findings related to Ivanti infrastructure, we encourage you to report them through one of the channels described in 'Reporting Channels'. Your watchful eyes and contributions are instrumental in safeguarding the security of our products and maintaining the integrity

of our infrastructure. We appreciate your commitment to enhancing Ivanti's security efforts. Thank you for partnering with us in this important endeavor.

In Scope

The vulnerability disclosure policy applies to any digital asset owned, operated, or maintained within Ivanti, including Ivanti’s products and services and Ivanti’s IT and OT infrastructure (including its systems and network).

Out of Scope

The following types of attacks are not considered part of our Vulnerability Disclosure Program:

- Denial of Service attacks, including resource exhaustion attacks, exploits causing denial of service, or any form of "resiliency testing" against Ivanti Corporate or Ivanti Hosted Solutions that could lead to service disruption.
- Physical testing of Ivanti Offices, Data Centers, Colocation facilities, etc.
- Social Engineering of our employees, customers, partners, etc.
- Any attack or event against an Ivanti product or solution hosted by a customer in their own network without prior approval for testing.
- Results from automated scanners.

Vulnerability Rewards

In addition to this Vulnerability Disclosure Program, Ivanti operates a specialized bugbounty program on Bugcrowd for selected Ivanti Products. This exclusive program is invitation-only, granting security researchers access to dedicated environments that host Ivanti Products.

If your vulnerability report affects a product within scope of Ivanti's bug-bounty program, your report will be moved to Ivanti's bug-bounty program, and you may receive a bounty award. Ivanti reserves the exclusive right to assess and qualify submissions for bounty rewards in its sole discretion.

Reporting Channels

If you have discovered a security vulnerability in any Ivanti enterprise software product or service, we encourage you to report it to us in a responsible and coordinated manner through one of these modes:

1. Easy to use Vulnerability Report Submission Form.
2. Email to responsible.disclosure@ivanti.com. Your report should include the following information:
    a. A detailed description of the vulnerability.
    b. Proof of Concept [PoC], if applicable.
    c. Steps to reproduce the vulnerability.
    d. Information about the affected product or service and its version.
    e. Your contact information, including your name, email address, and any additional contact details.

    If you wish to encrypt our communication, please use our PGP key here (Fingerprint: 5A86 C77C A361 B145 8A2C D672 DBF5 C7A9 FE96 C03D).

3. For general security inquiries, please write to security@ivanti.com.

Vulnerability Report Handling Procedure

- In response to your report, our VDP/bug-bounty partner, Bugcrowd will respond to you promptly, and work with you to understand and validate your report.
- Our security team will work to validate the vulnerability within ten business days after receiving it.

- Once the vulnerability is confirmed, Ivanti will prioritize its resolution based on the severity. We will provide regular updates to the reporter on the status of the remediation process.
- Ivanti will reserve and publish CVE(s) for vulnerabilities with CVSS score of 4.0 and greater, as calculated and validated by Ivanti's internal assessment process.
- We are committed to addressing and mitigating the reported vulnerability in good faith. We may seek input or assistance from the reporter as necessary.
- Ivanti may, from time to time, approve and make available more specific procedures for handling certain types of security vulnerabilities. Those additional procedures are extensions of this Vulnerability Disclosure Program.

Codes of Conduct

Play by the rules, including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail.

- Report any vulnerability you've discovered promptly.
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience.
- Use only the 'Official Channels' to discuss vulnerability information with us.
- Provide us with a reasonable amount of time (at least 120 days from the initial report) to resolve the issue before you disclose it publicly.
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information.
- You should only interact with test accounts you own or with explicit permission from the account holder; and
- Do not engage in extortion.

Legal Safe Harbor

To encourage research and responsible disclosure of security vulnerabilities, Ivanti will not pursue legal action against security researchers who make a good faith effort to comply with and report security vulnerabilities in accordance with this Vulnerability Disclosure Program.

Please understand that if your security research involves the networks, systems, information, applications, products, or services of a third party (which is not us), we cannot bind that third party, and they may pursue legal action or notify law enforcement. We cannot and do not authorize security research in the name of other entities, and cannot in any way offer to defend, indemnify, or otherwise protect you from any thirdparty action based on your actions.

You are expected, as always, to comply with all laws applicable to you, and not to disrupt or compromise any data beyond what our Vulnerability Disclosure Program permits.

Please contact us before engaging in conduct that may be inconsistent with or unaddressed by this policy. We reserve the sole right to make the determination of whether you made a good faith effort to comply with and report security vulnerabilities in accordance with this Vulnerability Disclosure Program, and proactive contact to us before engaging in any action is a significant factor in that decision. If in doubt, ask us first!

Vulnerability Report Submission Form

Please find our Vulnerability Report Submission Form (powered by Bugcrowd) below. In order to use the form, you need to accept third-party cookies by clicking "Enable Cookies". You can also find this form here.