Ivanti Bug Bounty Program

Contents

Introduction

The Ivanti Bug Bounty Program on Bugcrowd is focused solely on security issues in Ivanti products and solutions, including products and solutions of any company acquired by Ivanti (such as Pulse Secure and MobileIron) all together named under the same umbrella term of Ivanti products.

Ivanti products will be onboarded to the Bugcrowd platform at Ivanti's discretion. When a product is onboarded on the Bugcrowd platform that means a dedicated environment is created where security researchers can search for vulnerabilities. Only security researchers invited to the program have access to these environments.

The following products are currently onboarded to the Bugcrowd platform:

- Ivanti Neurons for MDM
- Ivanti Endpoint Manager Mobile (EPMM): on-premises version
- Ivanti Sentry: on-premises version
- Ivanti Neurons for ZTA (ZTA)

- Ivanti Connect Secure (ICS)
- Ivanti Policy Secure (IPS)

In addition to this general Ivanti Bug Bounty Program policy, each onboarded product has an individual Scope Policy. Individual product Scope Policies are available only to security researchers invited to the program. Security researchers in the program should make sure to read and completely understand the detailed Scope Policies for each individual product before attempting to find vulnerabilities in them.

We are actively working on onboarding more products into this program so stay tuned for new bounty opportunities!

This program enables you to responsibly disclose discovered vulnerabilities in any Ivanti product. We will review and handle all submissions, but please note only vulnerabilities affecting products that are onboarded to the program and are in scope for those products are eligible for bounty rewards

Response Targets

As it takes an effort to find a vulnerability, it also takes an effort to triage and remediate the vulnerability. We will make our best effort to meet the following response times:

Type of Response	Time to Response
First Response	2 Business Days
First Triage Feedback	2 Business Days (from first response)
Time to Triage	10 Business Days (from first response)
Time to Bounty	20 Business Days (from end of triage)

Depending on the severity of the vulnerability, response times could be shorter.

Throughout the triage and remediation, we will keep in contact with you providing status feedback.

Ratings/Rewards

For the initial prioritization/rating of findings, this engagement will use the Bugcrowd Vulnerability Rating Taxonomy. However, it is important to note that in some cases a vulnerability priority will be modified due to its likelihood or impact. In any instance where an issue is downgraded, a full, detailed explanation will be provided to the researcher - along with the opportunity to appeal, and make a case for a higher

priority. After considering any appeal, the final vulnerability severity will be determined by Ivanti.

More details are available in the full engagement brief, upon joining the program.

Program Scope

Testing is only authorized on the targets listed as in scope. Any domain/property of Ivanti not listed in the targets section is out of scope. This includes any/all subdomains not listed above. If you happen to identify a security vulnerability on a target that is not in scope, but it demonstrably belongs to Ivanti you can report it here. However, you should keep in mind that it is ineligible for rewards or points-based compensation.

If you are reporting a vulnerability on a product not onboarded on Bugcrowd platform, then:

- The decision on if a vulnerability type is in scope or out of scope for a given product will be done on a case-by-case basis solely at Ivanti's discretion, you can use this Policy and individual Scope Policies of onboarded products as guidelines for what not to report;
- Only in cases of a confirmed vulnerability reported in line with our reporting guidelines will we consider giving out rewards, however, final decision on if and what kind of reward will be given solely at Ivanti's discretion and decided on a case-by-case basis.

More details are available in the full engagement brief, upon joining the program

Engagement Rules

Your participation in the Ivanti Bug Bounty Program is voluntary and subject to the terms and conditions set forth in this Policy. By submitting a product vulnerability to Ivanti, you acknowledge that you have read and agreed to rules explained in this Policy.

Ivanti reserves the right to disqualify you from participating in the Ivanti Bug Bounty Program if you violate any rule specified in this program Policy.

Engagement Eligibility

To participate in Ivanti Bug Bounty Program, you must:

- Not be a resident of, or make your submission from, a country against which the United States has issued export sanctions or other trade restrictions;
- Not be in violation of any national, state, or local law or regulation;

- Not be employed by Ivanti, its subsidiaries or affiliates, or be a vendor or contractor working on behalf of Ivanti;
- Not be an immediate family member of a person employed by Ivanti, its subsidiaries or affiliates;
- Be 18 years of age or older.

Rules of Engagement

While searching for vulnerabilities in our products you must follow rules of engagement explained in this section. Failure to do so may result in being excluded from our bug bounty program.

- Abide by the program rules
- Researchers may not publicly or privately disclose any details whatsoever about reported vulnerabilities with a third party other than authorized Ivanti or Bugcrowd employees, without Ivanti's express written permission. For more information refer to the "Disclosure Policy" section
- Do not attempt to pivot in any way, elevate privileges or explore a system beyond the minimum necessary to prove vulnerabilities existence and impact. Do not use a vulnerability to compromise and exfiltrate data. Use a proof of concept only to demonstrate an issue
- Only interact with accounts and instances that you are authorized to use. Respect privacy of other users by making a good faith effort to avoid privacy violations
- Researchers are not authorized to engage in any activity that would be disruptive, damaging, or harmful to Ivanti, its brands or its users. This includes, but is not limited to, social engineering (phishing, vishing, smishing, etc.), physical and denial of service attacks against users, employees, or Ivanti as a whole
- Do not interact with any physical location related to Ivanti included, but not limited, to offices, data centers or employees' locations

Reporting Guidelines

For all submissions, please include:

- Detailed technical description of the vulnerability being reported;
- Reproducing focused step-by-step explanation of vulnerability's discovery and exploitation where applicable, and each step must contain appropriate evidence, such as:
    - Screenshots and/or videos;
    - Exploit code such as CLI commands, snippets of code or full working PoC exploit scripts;

    - Network traffic such as logs, HTTP requests and responses, packet dumps etc.;
    - Activity identification information such as:
    - Test account information, such as email and usernames / user IDs;
    - IP information, such as source IP addresses from where attacks were sent or destination IP addresses for any achieved callbacks;
    - Timestamps including time zones;
    - Filenames and their hashes;
    - Any other custom identification, such as custom HTTP header names and values;
- Clear demonstration of security boundary breach such as:
- Any and all data that was accessed;
- Capabilities achieved;
- Your evaluation of vulnerability's ease of exploitation and impact;
- Recommendation on how to fix the vulnerability, which includes generic advise for a vulnerability as well as specific advice for the reported instances of vulnerability and associated technologies that Ivanti uses;

A direct scanner output or scanner generated reports, as well as outputs of exploitation tools, without following the above reporting guidelines will not be accepted as valid submissions. If your tool detects a vulnerability, please confirm it manually and provide evidence using those manual steps. Scanner and tool output can then be added to report as accompanying evidence, but they will not be accepted as standalone evidence.

Please report only one vulnerability per submission unless there is a need to chain vulnerabilities to demonstrate security impact.

Quality of your submission will directly impact the speed of the triage as well as correctness of reward decision. Failure to follow the reporting guidelines could result in Ivanti not recognizing the existence of vulnerability or its impact and you missing out on your bounty.

Out of Scope

Please refer to each product's individual Scope Policy for additional product-oriented description of the scope.

Out of scope vulnerabilities for all Ivanti products are:

1. Rate limiting, DoS or DDoS vulnerabilities;
2. Vulnerabilities that only demonstrate lack of security best practice without actual security impact such as but not limited to:
    a. Weak configured SSL/TLS services;

    b. Missing or weakly configured security headers such as, but not limited, to:
        - Content Security Policy;
        - Strict-Transport-Security;
        - X-Frame-Options;
        - X-Content-Type-Options;
        - X-XSS-Protection;
        - Referrer-Policy;
- Missing HTTP cookie flags such as HttpOnly, Secure and SameSite;
- Supporting HTTP methods such as TRACE;
- Host header injection;
- Weak password policy;
- Missing or weak email authentication methods and protocols such as SPF, DKIM and DMARC;
- Missing certificate pinning;
- Missing autocomplete directive on HTML forms;

3. Information disclosure such as, but not limited, to:
    a. Software name and version disclosure;
    b. Descriptive error messages;
    c. Stack traces;
    d. Known public files or directories;
4. User enumeration;
5. CSRF on unauthenticated actions or actions with minimal impact such as login and logout functionalities etc.; vulnerabilities that require hard prerequisites such as, but not limited, to:
    a. Man-in-the-Middle access;
    b. Physical access;
    c. Rooted devices;
    d. Outdated operating systems;
6. Vulnerabilities that require unlikely user interaction such as, but not limited, to:
    a. Self-XSS;
    b. Clickjacking;
    c. Tabnabbing;
    d. Disabling security controls;
    e. Content spoofing and text injections;
7. CSV and Excel injections without demonstrating security impact;
8. Open redirect unless additional security impact can be demonstrated, such as loss of sensitive data;
9. Unrestricted file uploads with only resource consumption impact;
10. Vulnerabilities on third-party software such as frameworks, plugins, or libraries unless security impact can be demonstrated;
11. Vulnerabilities that have had an official patch for more than 2 months will be awarded on a case-by-case basis;

12. Vulnerabilities only affecting users of outdated and unpatched client software, such as browsers (more than two stable versions behind the latest released stable version), spreadsheet viewers, deprecated technologies (such as Flash) etc. will be awarded on a case-by-case basis;
13. If a product is hosted in cloud environment (AWS, Azure, GCP etc.), then any vulnerability found in cloud environment infrastructure is out of scope;
14. Unless specifically stated in the product Scope Policy, any vulnerability found in client and desktop applications are by default considered out of scope;
15. Any vulnerability related to environment where a product is hosted:

- Vulnerabilities on hosts such as, but not limited, to:
    - Out of date software;
    - Restricted shell escapes;
    - Open ports;
    - Unnecessary exposed services;
- Vulnerabilities on network devices;

If a vulnerability that is out of scope can be chained with an in-scope vulnerability, please mention this in the submission report as it may help you demonstrate higher impact and earn you a better reward.

Engagement Changes

The Ivanti Bug Bounty Program policy, including individual product Scope Policies, are subject to change or cancellation by Ivanti at any time, without notice. As such, Ivanti may amend its policies at any time by posting a revised version. By continuing to participate in the Ivanti Bug Bounty Program after any such changes, you accept the policies, as modified.

Security Advisories and CVEs

The purpose of Security Advisories and CVEs is to communicate to our customers any product vulnerabilities, the severity, and mitigation steps. Decision to publish a Security Advisory or to request a CVE will be done solely at Ivanti's discretion on a case-by-case basis. This decision will be done not only based on the reported vulnerability's severity, but also on customer specific information available only internally to Ivanti.

Disclosure Policy

No details from this program should be disclosed publicly or privately without express written consent from Ivanti. This includes, but is not necessarily limited, to:

- Any details from individual product Scope Policies;

- Contents of any submission and details about security issues and vulnerabilities regardless of their status (open, resolved, duplicate etc.); your communication with Ivanti related to the program, such as discussions about the scope, individual submissions, rewards etc.; knowledge and information about the products gained through participation in the program

In addition to guidelines stated in this program, Bugcrowd's disclosure guidelines should be followed.

Safe Harbor

Security researchers who make a good faith effort to comply with this posted disclosure policy will be considered authorized Ivanti testers. Ivanti will make an equally good faith effort to work with security researchers who report issues under this program. If legal action is initiated by a third-party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Ivanti reserves the right to seek legal action against individuals who do not work within this policy and break ToS, EULAs, or local laws and regulations. Individuals who report potential issues under multiple programs without first receiving clearance from Ivanti will not be considered to be operating under this policy

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please inquire through the Bugcrowd Support Portal before going any further.