ivanti

Ivanti's Responsible Disclosure Policy

Ivanti, Inc.

contact@ivanti.com

+1-888-253-6201

www.ivanti.com

Owner: Chief Security Officer

Applicable country: Global

Last revision: January 2022

Approved by: Ivanti Security Council

Ivanti's Responsible Disclosure Policy

Ivanti is committed to maintaining secure products and infrastructure for our customers and for the benefit of the community. Ivanti appreciates and supports the efforts of the security community who help us maintain that commitment by reporting potential issues to us.

Our Responsible Disclosure Policy applies to all Ivanti products and Ivanti networks, including products and networks companies acquired by Ivanti. Some Ivanti products are covered under a Bug Bounty program (as indicated below).

Reporting

For all issues with Ivanti Product or Solutions, including products of companies acquired by Ivanti (such as Pulse Secure and MobileIron Products), please report issues through our HackerOne.

- https://hackerone.com/ivanti/

For issues with Ivanti infrastructure and all other non-product reports, please contact us through our Responsible Disclosure email.

- Responsible.Disclosure@ivanti.com

If you are concerned about the sensitivity of the information you want to share, you can:

- Use our PGP key here for your use (Fingerprint: 5A86 C77C A361 B145 8A2C D672 DBF5 C7A9 FE96 C03D). If you want to verify the fingerprint, please email us.
- You can email us at the above address and request an O365 encrypted email thread to be started.

We ask that you please provide a high-quality report, including a Proof-of-Concept. If you performed your test against an internet facing system, we ask that you provide the IP address you performed the test from so we can quickly validate your activities.

Scope Exclusions

The following type of attacks are not considered to be part of our Responsible Disclosure Program:

- Denial of Service attacks, including resource exhaustion attacks, exploits which cause denial of service, or other types of "resiliency testing" against Ivanti Corporate or Ivanti Hosted Solutions that could lead to disruption of services.
- Physical testing of Ivanti Offices, Data Centers, Colocations facilities, etc.
- Social Engineering of our employees, customers, partners, etc.
- Any attack or event against an Ivanti product or solution that is hosted by a customer in their own network without prior approval to perform testing.

In addition to the above, the following vulnerabilities and weakness are out of scope:

- Clickjacking on pages with no sensitive actions or without impact.

- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions.
- Attacks requiring MITM or physical access to a user device, application, or environment will be reviewed on a case-by-case basis.
- Previously known vulnerable libraries without a working Proof of Concept.
- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing best practices in SSL/TLS configuration, including weak ciphers.
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS.
- Rate limiting or bruteforce issues on non-authentication endpoints.
- Missing best practices in Content Security Policy.
- Missing HttpOnly or Secure flags on cookies.
- Missing email best practices such as Invalid, incomplete, or missing SPF/DKIM/DMARC records.
- Vulnerabilities only affecting users of outdated or unpatched browsers or operating systems.
- Software version disclosure or Banner identification issues.
- Tabnabbing.
- Open redirects, unless an additional security impact can be demonstrated.
- Public zero-day vulnerabilities that have had an official patch for less than 1 month will be reviewed on a case-by-case basis.

What to expect from Ivanti

In response to your report, Ivanti will:

- Reply to you within two business days to let you know we received your report.
- Confirm whether your report is an issue two business days after confirmed receipt.
- Provide you a report on how we'll fix it and when we'll fix.
- Let you know when it's been fixed.
- Release a public report where appropriate. Reporters who follow the responsible disclosure policy may be publicly credited.

For reporters who report previously unknown issues, we send Ivanti Swag as a thank you!

Ivanti's Bug Bounty Program

Ivanti is proud to include a HackerOne bug bounty program for:

- Pulse Connect Secure product
- MobileIron Core product

- Please see the HackerOne program for more details: https://hackerone.com/ivanti/

The Bug Bounty Program operates within this responsible disclosure policy (including the above exclusions) and bounties are rewarded based on the severity of the vulnerability and the quality of the report.

Other security issues reported that have been validated will be rewarded with Ivanti Swag. Please do not ask for other payment.

Safe Harbor and Legal

Researchers who make a good faith effort to comply with this posted disclosure policy will be considered authorized Ivanti testers. Ivanti with make an equally good faith effort to work with 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. Ivanti does not recognize other responsible disclosure policies, timelines, programs, or frameworks that are not covered by this policy. Individuals who report potential issues under multiple programs without first receiving clearance from Ivanti will not be considered to be operating under this policy.

Questions

If you have any issues with the above methods or you have questions, you can reach the Ivanti Information Security team at security@ivanti.com.

1.0 Revision History

Version	Date of Change	Responsible	Summary of Change
1.0	2018	Information Security	Creation
1.1	2022	Information Security	Updated Policy