# Product Incident Response and Vulnerability Communication Plan Summary

## Overview

Ivanti's vulnerability management program is a central part of our commitment to security. Our top priority is upholding our commitment to deliver and maintain secure products, while practicing responsible disclosure protocols. We employ rigorous testing and validation methodologies to enable swift detection, patching, and disclosure of vulnerabilities in collaboration with the broader security ecosystem. Ivanti's Product Incident Response and Vulnerability Communications Plan Summary outlines how we will ensure that our customers and partners are aware of vulnerabilities and are empowered to defend their environments when vulnerabilities arise.

Ivanti's Product Incident Response Plan and our Vulnerability Communication Plan has been developed with the protection and support of our customers in mind. It is important for customers to have access to accurate information so they can assess the risk of vulnerabilities, understand steps for mitigation, and have the time to plan and act to protect their environments from threat actors. This is a summary version of the internal documentation used at Ivanti and is provided to ensure transparency with our customers and partners.

## How does Ivanti determine the impact of a vulnerability?

We believe that responsible CVE disclosure from a vendor is a sign of a healthy code analysis and testing community, and an important part of software maintenance. We also acknowledge that the CVSS score does not always reflect the true nature of the risk to a customer's environment or the current threat landscape.

When our Product Security team assesses vulnerabilities, we go beyond the CVSS Version 4.0 base score. Additional factors we consider when determining the impact and risk of vulnerabilities to our customers include, but are not limited to:

- Active exploitation
- Ease of exploitation
- Intended deployment model (edge, etc.)
- Privilege requirements
- Potential for harm
- Proof of concept (POC) availability
- Default and recommended configurations

## What vulnerabilities will we communicate?

Ivanti will issue communications for any vulnerability in Ivanti code scored by Ivanti's Product Security team with a CVSS Version 4.0 base score greater than a 4.0.

Ivanti will communicate resolution of vulnerabilities in Open Source or Third-Party library code through Product Patch Notes and/or SBOMs. Ivanti will only use Security Advisories for Open

Source or Third-Party library code if there is confirmed or a high risk of exploitation. On a case-by-case basis we may also choose to inform customers and partners that our products are not impacted by Open Source or Third-party library vulnerabilities or significant industry events to clearly inform customers there are no actions required to keep their installation secure.

## How and when will we communicate vulnerabilities?

When vulnerabilities occur, we will post a publicly available Security Advisory in our Ivanti Community for each release that resolves at least one vulnerability that meets the criteria described above.

In the case of an actively exploited Zero-day vulnerability, Ivanti will issue communication as soon as a fix or mitigation is available for customers.

Ivanti generally discloses standard security patches on the second Tuesday of every month to provide a predictable schedule for our customers and allow them to better allocate time and personnel efficiently for the timely updates.

In the case of vulnerabilities that have confirmed exploitation of one or more customers, or it is a vulnerability that we believe could have a high likelihood of customer exploitation, we may use additional communication methods to ensure customers are informed and can act expeditiously, including:

- Email communication to technical, security, and/or privacy contacts in our customer account records.
- Phone calls from the Ivanti Account team members.
- Coordinating with CERTs and Security Partners to amplify our communications.

### Early notification

In some situations, and at the discretion of Ivanti, we may also provide early notification of vulnerabilities to our Industry Security and Intelligence Sharing Partners, our Managed Service Provider Partners, our OEM partners and any partner for which Ivanti knows hosts and manages the Ivanti Product for downstream customers. This may include access to early fixes.

*Early notification is not guaranteed and will not be done at the expense of broader customer security.*

For technology partners which OEM one or more Ivanti solutions we will provide, on a best effort basis, early notification to allow the necessary time for them to apply the update to their own solution.

For other partners beyond those described above, we will provide specific resources in the Partner Portal to help them communicate with customers shortly before public release of the vulnerability.

Ivanti does not provide any customers with direct early notifications for vulnerabilities unless we have a reason to believe there is a risk to life or personal safety.

## What information will communications contain?

Ivanti communicates vulnerabilities on our customer forum in a Security Advisory, which will contain at a minimum:

- The product(s) and affected versions.
- The CVE Number and the CVSS Score for each vulnerability (if applicable).
- A description of the vulnerability that includes appropriate language for the Common Weakness Enumeration (CWE) of the vulnerability.
- Any additional action necessary to remediate the vulnerability (i.e. performing patching or changing configuration).
- Any temporary mitigations that customers can perform to reduce the impact or likelihood of exploitation.
- If the vulnerability has been exploited based on Ivanti's knowledge at the time of publish or update.
- If a detailed Proof-of-Concept (PoC) is publicly available to Ivanti's knowledge at the time of publish or update.
- A link to a KB article (if applicable).

Knowledge Base Articles (when needed) will contain:

- Additional information that will assist customers in protecting or assessing the risk to their environment.
- How to receive notification for future updates to the Knowledge Base article.

Ivanti will never share detailed information about the vulnerability, such as a proof of concept (POC) or information that would help anyone exploit our products.

Security Advisories and Knowledge Base articles may be updated if new, and relevant information becomes available for supported versions.

## Other important communication topics

### CVE Number Authority (CNAs)

Ivanti is now a CVE Numbering Authority. Ivanti previously published CVEs through HackerOne, which we still use for our Public Vulnerability Disclosure Program. A CVE published through HackerOne does not necessarily mean the vulnerability was discovered publicly.

### Mitigations

We understand that deploying patches or new software versions is time-consuming and can impact business operations for many organizations. Ivanti cannot guarantee the availability of mitigations but will always try to provide customers with information to help plan their updates.

Please note that mitigations may require additional security controls or technologies that Ivanti doesn't provide. It may also limit the capabilities and functions of the product.

Mitigations are temporary measures to allow customers time to patch and may not be complete or could potentially be circumvented with additional effort. Ivanti always advises that customers deploy the fix provided to ensure their environment is protected.

### Indicators of Compromise (IOC) and Detection Guidance

For vulnerabilities that have been publicly exploited and are high-risk, Ivanti will strive to provide detection and analysis guidance for exploitation. Our Technical Support teams will share

detection and analysis guidance with customers that have confirmed impact to move customers forward in their forensics investigation.

During the course of an investigation, we may work with law enforcement, other customers, and third-party experts to quickly address vulnerabilities and provide remediation. Some of the information that Ivanti receives cannot be shared with customers because it is designated confidential, follows traffic light protocol (TLP), or because it would impact the effectiveness of the investigation.

**Communication about vulnerabilities in unsupported versions**

Ivanti does not communicate or publish information about vulnerabilities in unsupported versions of our products or products that are end of life. Ivanti only assesses the exploitability of products that are currently supported.

At Ivanti's discretion, we may publish information about active exploitation of older products or versions in extraordinary circumstances.

You can see the current supported version of Ivanti Products here: https://www.ivanti.com/support/product-documentation

You can see the products which have been announced as End of Life here: https://forums.ivanti.com/s/article/End-of-Life-Policy-for-Ivanti-Products-Landing-Page?language=en_US

**Credit**

Ivanti will publicly credit researchers who identify vulnerabilities in our product and participate in our Responsible Disclosure Program. More details about eligibility and requirements can be found in the Responsible Disclosure Policy.

## Additional resources

Ivanti's Responsible Disclosure Policy – https://www.ivanti.com/support/contact-security

Ivanti's Security and Compliance Page – https://www.ivanti.com/resources/security-compliance

## Revision History

| Version | Date of change | Summary of change |
|---|---|---|
| 1 | 2025.0218 | Policy Published |