Vulnerability Disclosure Policy

Our team works vigilantly to protect our customers and their information assets impacting by our software. We recognize the important role that security researchers and our user community play in keeping Kaseya and our customers secure. If you discover a site or product vulnerability please notify us using the guidelines below.

To encourage responsible disclosure, we commit that if we conclude that a disclosure respects and meets all the guidelines outlined below we will not bring a private action or refer a matter for public inquiry.

We strongly encourage anyone who is interested in researching and reporting security issues to observe the simple courtesies and protocols of responsible disclosure.

Guidelines for responsible disclosure

- Share the security issue with us before making it public to peers, on message boards, mailing lists, and other forums.
- Allow us reasonable time to respond to the issue before disclosing it publicly.
- Provide full details of the security issue, and be open to describing how you found it so we may reproduce the conditions.
- Understand that many services we use are not under our control. Reporting vulnerabilities in Azure Websites (think header info), TyepPad or HubSpot will be forwarded to the corresponding partner companies. We will not be triaging such cases past that.

Do not engage in security research that involves

- Potential or actual denial of service of Kaseya applications and systems.
- Use of an exploit to view data without authorization, or corruption of data.
- Requests for direct compensation for the reporting of security issues either to Kaseya, or through any external market-place for vulnerabilities, whether black-market or otherwise.

Report security vulnerabilities to

- security@kaseya.com.

Be sure to include an email address where we can reach you in case we need more information.

We take security issues seriously and will respond swiftly to fix verifiable security issues. Some parts of our product are complex and take time to update. When properly notified of legitimate issues, well do our best to acknowledge your emailed report, assign resources to investigate the issue, and fix potential problems as quickly as possible.

Bug Bounty

Kaseya does NOT offer compensation for vulnerabilities that are disclosed. We will, from time to time, say thank you for new and interesting reports in our thanks section of this page. Please note however that providing a report does not guarantee a credit.

Thanks!

Thanks for helping to keep Kaseya community safe. We really appreciate the effort!

Below is a list of security researchers (in alphabetical order) who have participated in our responsible disclosure program.

- Ehraz Ahmed
- Aditya Agrawal
- Ishan Anand
- Narendra Bhati
- Mayank Bhatodra and Parveen Yadav
- Mike Czumak
- Chiragh Dewan
- Javid Hussain
- Peter Jaric
- Osanda Malith
- Murugesh
- Ajay Singh Negi
- Sandeep Singh Rehal
- Sahil Saif
- Kamil Sevi
- Muhammad Shahmeer
- Danish Tariq and Noman Ramzan
- Jigar Thakkar
- Jay Turla
- Mohankumar Vengatachalam
- Adam Ziaja