Kaspersky's ethical principles in Responsible Vulnerability Disclosure

kaspersky BRING ON THE FUTURE

Learn more on
www.kaspersky.com

Our society is rapidly changing, and technology is becoming ever more crucial a part of our lives in digitalizing every aspect of our day-to-day experience. The complexity of technology makes vulnerabilities and failures inevitable. Still it is we, humans, who develop the technology and we who make use of it, and it is our responsibility to plan for this contingency. We firmly believe that inevitable failures in technology development must be fixed.

Responsible Vulnerability Disclosure (RVD) as a process not an event, serves an important indicator of Kaspersky's commitment to product quality and 'compensates for this inevitability'[1]. As part of the global cybersecurity ecosystem, we work with vendors, researchers, users and other stakeholders for the mutual benefit of the ecosystem and society at large.

In all cases, we put the safety and security of our users (people and organizations using Kaspersky products and solutions) first, and hence cooperate with affected vendors – individuals or organizations that created and/or maintain the product where a vulnerability is found, and other possible victims. For this we are guided by the ethical principles of Responsible Vulnerability Disclosure, which underlie our internal policies and processes to ensure that we act in a transparent, responsible and consistent manner.

#1
Build trust

For us, trust comes first. It is the foundation of any human relations, and for cybersecurity trust is essential: cybersecurity not only requires trust – it depends on it. We acknowledge the crucial value of trusted relations between parties for responsible vulnerability disclosure. For this, we pledge to continue:

- prioritizing interests of users and society at large, while acknowledging the sensitive issues and risks involved in responsible vulnerability disclosure;
- reporting all vulnerabilities found and communicating them to vendors in a responsible manner[2];
- behaving in a transparent and predictable manner toward other actors of the process, including security researchers, CERTs, government authorities and the general public;
- presuming benevolence as a motive for all parties, while taking the time and effort to coordinate actions and reduce any harm of vulnerability.

#2
Inform the affected party first

Responsible Vulnerability Disclosure as a complex process can face numerous obstacles: sometimes it is difficult to reach a vendor or company; participants in the process may stop responding due to other priorities; and no one is safe from information leaks – whether intentional or not. Despite these issues, we pledge to continue:

- informing affected vendor(s) first whenever possible and initiating cooperation with them to assist in developing patches and remediation plans in order to reduce harm and minimize exposure risks, while taking steps to protect our own users from the given threat;
- providing evidence-based, timely and targeted reporting to enable all parties involved to make better informed decisions and take action;
- clearly communicating steps of RVD to all parties involved.

1 The CERT Guide to Coordinated Vulnerability Disclosure https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.
2 This step needs to be read as part of the RVD separate from and preceding public disclosure of a vulnerability.

#3
Coordinate efforts

Coordination plays an important role in vulnerability disclosure, especially in multi-party cases due to the growing interdependency of the global supply chains. We pledge to continue:

- cooperating with a range of external stakeholders while following industry's developed best practices, including ISO/IEC 29147:2018 on vulnerability disclosure;
- allowing sufficient time for all parties involved in a case to analyze the vulnerability or incident and start working on remediation;
- calling for a coordinated multi-stakeholder response effort, with the inclusion of the independent research community.

#4
Maintain confidentiality where appropriate

The irresponsible or uncoordinated release of information on a vulnerability's technical details can assist malicious actors in their making use of it and, thus, put users at a greater risk. Our main goal is to protect our users; therefore, we will report a vulnerability to the affected vendor in a secure manner. However, if the vendor does not respond or does not take measures needed to eliminate the vulnerability within a reasonable timeframe, and also depending on the severity and scale of the risk from the vulnerability to users and society, we must inform our users and all other users about the threat associated with it. For these reasons, we pledge to continue:

- sharing necessary information in a confidential manner with parties that need to develop mitigation measures first;
- working through the most trusted and secure communication channels for reporting to ensure that data directly relevant to an incident and its remediation is handled in accordance with applicable laws, contractual obligations, and respect for privacy of the parties involved;
- negotiating disclosure's terms and conditions with the vendor in accordance with local regulations, laws, and the vendor's policies regarding vulnerability disclosure;
- if the vendor does not reply, depending on the severity and scale of the vulnerability and immediacy of the risk, making the disclosure through our own communication channels and disclosing the information in accordance with our internal policies, local regulations and industry's best practices, while keeping the vendor informed about this intention.

#5
Incentivize desired behavior

Industry, states, and users, broadly speaking, are increasingly aware of RVD's importance, but still there is a lot to do to agree on common definitions and develop an industry-shared mindset. Meanwhile, we believe it is important to incentivize responsible behavior, and for this we pledge to continue:

- raising awareness to enhance cyber-consciousness among all parties and make sure remediation and patches are developed and applied timely;
- continuously supporting and commending actors who take responsible steps to discover, report and remediate any vulnerabilities in their products.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them.

Learn more at www.kaspersky.com.

www.kaspersky.com

kaspersky

Enterprise Cybersecurity: www.kaspersky.com/enterprise
TechnoWiki: www.kaspersky.com/technowiki
IT Security News: www.kaspersky.com/blog
Cyber Threats News: www.securelist.com