VULNERABILITY DISCLOSURE POLICY

At Rolls-Royce the security of our systems and our customer data together with the safety and continuity of product and service delivery, are a top priority.

To help maintain the integrity, reliability and confidentiality of Rolls-Royce's assets we encourage responsible reporting of potential / actual vulnerabilities or threats to Rolls-Royce data, systems, products, services or networks.

By actively reporting vulnerabilities or threats you are helping to maintain the safety and reliability of our systems.

How to Report a Vulnerability

This Vulnerability Disclosure policy only applies to vulnerabilities in Rolls-Royce's data, systems, products, services or networks. If you believe you have discovered a vulnerability in any of these assets or have a security incident to report, that is in-scope for the purposes of this Vulnerability Disclosure policy, please contact us by emailing responsible.disclosure@rolls-royce.com making sure that you adhere to the Guidelines for Engagement, set out below.

If you wish to encrypt your message please use this PGP key, which will help protect any sensitive details in your email such as how to reproduce the vulnerability. The key can be copied to your local device and then imported in to your PGP application.

Guidelines for Engagement

Please ensure that you report any vulnerability or threat in accordance with the following guidelines:

- Report the vulnerability or threat as quickly as is reasonably possible to minimise the risk of hostile actors finding and taking advantage of it.

- Safeguard the confidentiality of the discovery so that others are not able to gain access to the information.

- Do not engage in any activity that violates any applicable laws and regulations in any country where Rolls-Royce data, products, services, systems or networks reside or where data traffic is routed, including any federal or state laws or regulations.

- Do not engage in any activity that can or could cause harm to Rolls-Royce, our customers or our employees.
- Do not engage in any activity that can or could stop or degrade Rolls-Royce's systems, products, services, network or any other assets.
- Do not use any techniques that can influence the availability of our online services.
- Do not make any changes to Rolls-Royce systems.
- Do not modify or delete any Rolls-Royce data.
- Do not copy any Rolls-Royce data unless strictly necessary for your investigation and if necessary, treat such data as confidential and use at least the same level of care as if it were your own, implementing reasonable measures to prevent unauthorised access. When you no longer require the Rolls-Royce data for the investigation you must immediately destroy it.
- Do not make any customer or business data public.
- Do not create a backdoor in any Rolls-Royce system.
- Do not utilise a vulnerability further than is necessary to establish its existence.
- Do not attempt to penetrate the system more than required and if you successfully penetrate the system do not share any gained access with others.
- Do not use any invasive or destructive techniques, including any brute force techniques, in the course of your investigations.
- Do not use social engineering in order to gain access to Rolls-Royce's systems.

Please do not ask Rolls-Royce to compensate you for your report.

If at any time you are unsure if your intended or actual actions are acceptable please contact Rolls-Royce's Cyber Security Team, via responsible.disclosure@rolls-royce.com for guidance and you can use the PGP key if you so wish, to protect any sensitive details.

Information Required

To help us evaluate your discovery as efficiently as possible, please provide the following information:

- Description of the vulnerability or threat.
- Details of how it was discovered and the steps you took.
- Evidence of the findings, which may include screenshots, proof of concepts, video, etc.
- Details of the affected or potentially affected data, system, product, service or network.
- Details of the potential impact.
- Whether you would like to be advised once the vulnerability has been resolved.
- Your contact details.
- Any additional relevant information.

Out-of-Scope Vulnerabilities

Certain reports and vulnerabilities are considered out-of-scope for the purposes of this Vulnerability Disclosure policy, as follows:

- Phishing attempts
- CSP vulnerabilities; SSL/TLS best practices
- Denial of service attacks (DDoS)
- Resource exhaustion attacks
- Fake/replayed CAN message
- Non-reproducible vulnerabilities
- Self-XSS and other vulnerabilities only possible through Self-XSS
- Physical testing
- Social engineering, including attempts to steal cookies, fake login pages to collect credentials
- Reports on vulnerabilities generated by automated scan tools
- Reports on publicly available information and/or browser instructions

What Happens Next?

Rolls-Royce will acknowledge receipt of your email as soon as reasonably possible, typically within 72 hours. The response may include a request for additional information to enable secure communication and will confirm if the discovery is out-of-scope or a duplicate report.

Please be advised that priority for bug fixes or mitigations is assessed by looking at impact severity and exploit complexity and that some submissions may take longer to address than others, so please allow us enough time to fix the vulnerability or issue before sharing with a third party or making any information public.

If you would like to be advised once the vulnerability has been resolved, then we will strive to do so as soon as possible following resolution. We ask that you securely delete any and all data retrieved during your research as soon as it is no longer required or within one month of Rolls-Royce resolving the vulnerability, whichever is the first to occur.

Your Privacy

Personal data that Rolls-Royce receives in connection with your submission will be retained and protected in accordance with Rolls-Royce's Privacy Policy.

If you would prefer not to provide your name and contact details, then please be aware that without this information we will be unable to discuss next steps with you.

Feedback

If you wish to provide feedback or suggestions on this policy and the disclosure handling process, please do so by contacting responsible.disclosure@rolls-royce.com. We welcome input to ensure that during the natural evolution of this Vulnerability Disclosure policy it remains clear, complete and relevant.

Legalities

This Vulnerability Disclosure policy is designed to be compatible with common good practice among well-intentioned individuals. It does not give you permission to act in any manner that is inconsistent with the law or which causes Rolls-Royce to be in breach of any of its legal obligations.

By responsibly submitting your findings to Rolls-Royce and where you have acted in good faith and in accordance with this Vulnerability Disclosure policy, Rolls-Royce affirms that it will not pursue legal action against you. Rolls-Royce reserves all legal rights in the event of noncompliance with this Vulnerability Disclosure policy.

Alternative Reporting

If you do not wish to make a report directly to Rolls-Royce, please report issues to the National Cyber Security Centre (NCSC). For more information on how to do this is available on the NCSC vulnerability-reporting page at: https://www.ncsc.gov.uk/information/vulnerability-reporting.

Please contact us here for correspondence unrelated to issues concerning security, vulnerabilities or threats.

This information is provided by Rolls Royce in good faith based upon the latest information available to it; no warranty or representation is given; no contractual or other binding commitment is implied.