Notice to Suppliers

Cyber Security information relating vulnerabilities reported by the UK National Cyber Security Centre

Originator: Neil Cassidy
Job Title: Director Cyber Security, Rolls-Royce plc
Business Unit: IT Risk & Compliance

NTS Number: 475
Issue: 1
Date: 26 October 2019

For the attention of the Managing Director and the Head of IT or IT Security.

Scope/Applicability:

All Rolls-Royce plc suppliers.

Dear supply partner,

Introduction:

Rolls-Royce has been informed of an on-going investigation led by the UK National Cyber Security Centre (NCSC) which has identified an Advanced Persistent Threat (APT) group actively targeting vulnerabilities affecting Virtual Private Network (VPN) products from vendors Pulse Secure, Fortinet and Palo Alto.

The NCSC report which contains all the latest information can be found on their website: https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

This activity is ongoing, targeting both UK and international organisations. Affected sectors include government, military, academic, business and healthcare. These vulnerabilities are well documented in open source, and industry data indicates that hundreds of hosts may be vulnerable.

This document is intended to remind you that you are a potential target of these APT groups and to share some information that may help you to identify areas of vulnerability, and what to do to reduce the risk. Much of this information is directed to cyber security activity that all companies should undertake and enforce, and you will no doubt already be undertaking much of this activity.

This information is designed for your IT or IT Security department and should be forwarded to them. Of course, your company remains solely responsible for implementing and monitoring security arrangements to fulfil its contractual and regulatory obligations. Whilst Rolls-Royce hopes that you will find this document useful, it is not intended to constitute advice on your company's IT security arrangements or to suggest that the implementation of the measures outlined will in itself be sufficient to ensure adequate levels of security.

What action to take:

In order to combat an attack against your VPNs, we strongly recommend that suppliers;

- Identify if your company utilises any of the affected VPN products (Pulse Secure, Fortinet and Palo Alto)
- Patch the affected VPN product to address the identified security vulnerabilities (as detailed in the NCSC report)
- Reset authentication credentials associated with affected VPNs and accounts connecting through them
- Investigate your company logs for evidence of compromise, especially if it is possible that patches were not applied immediately after their release (steps for each VPN product detailed in the NCSC report)
- Search for evidence of compromised accounts in active use, such as anomalous IP locations or times
- Where possible, enable two-factor authentication for the VPN to defend against password replay attacks

If you have detected successful exploitation of the VPN product, we recommend suppliers to;

- Check all configuration options for unauthorised changes. This includes the SSH authorized_keys file, new iptables rules and commands set to run on connecting clients.
- Continue to monitor logs for the VPN, network traffic and services users connect to through the VPN such as email. Check for connections from uncommon IP addresses, particularly those with successful logins or large data lengths returned. Identify replay attempts using old credentials that have been reset.
- Resetting authentication credentials will defend against unauthorised access using credentials acquired prior to patching affected systems.
- **If you process Rolls-Royce information or connect to Rolls-Royce IT systems, please contact Rolls-Royce Security Operations at uk.soc@rolls-royce.com or +44 (0) 1332 622800**

Any current activity related to these threats should be reported via the NCSC website where the NCSC can offer help and guidance.

NTS Category:	**Authorised by:**
General Information / Communication	Neil Cassidy Director Cyber Security, Rolls-Royce plc