SERVICE DESCRIPTION

Support Update Service (SUS)

Name	Support Update Service (SUS)
Owner	TSS
Status	APPROVED
Classification	UNCLASSIFIED-INTERNAL
Version	V2.0
Date	14 March 2018
Review	14 March 2019

Contents

1 Introduction

The Support Update Service (SUS) the aim is to disseminate important technical and support information to customers and NTT Ltd. employees. It is a value-add service provided by the NTT Ltd. EU-SOC.

A range of sources are monitored by the Technical Security Services (TSS) Team including mailing lists, checking websites etc. The Team will then decide if an advisory is required and will then write and release one. TSS Management will write and release advisories regarding internally-provided services (such as Portal maintenance, or any Service outage related issue e.g. Telephone)

2 Products/Vendors covered under SUS

Core Vendors/Products under SecureCall are eligible for SUS messages. This currently includes:

- Blue Coat
- Check Point
- F5
- Fortinet
- Juniper
- Palo Alto

3 Types of SUS Advisories

SUS alerts are sent for issues and updates related to Products under SecureCall, such as:

- Vulnerabilities, proven to affect Technology
- Common product problems, critical in impact
- Version updates*
- Support updates

*SUS does not cover 'routine' bulletins such as Anti-Virus or IDP signature updates.

3.1 Vulnerabilities

An advisory is generally sent if an alert is received which refers to a significant vulnerability in a supported product, such as serious threat or exploit, or for a virus, which a significant number of our customers may be susceptible to.

- A vulnerability advisory should contain:
- A very brief summary of the threat/vulnerability
- A statement from the supplier
- location of hotfixes or patches
- Description of any mitigating configuration changes that can be made. The description may take the form of a tech note. If the changes require significant then a step by step guide should not be attempted, and advice should include 'if you would like Support from an NTT Ltd. Engineer to make these changes, please contact your account manager' or 'please contact the support line for further information'.

3.2 Product Problems

If the SOC becomes aware of significant or re-occurring issues with products that could affect a large number of customers then an advisory may be sent. This would apply to temporary product issues, such as updates failing, serious configuration issues that could cause problems or affect security or significant bugs in the product where workarounds are available. An advisory will be sent to customers after assessment of impact and how common the fault would be across the customer install base.

3.3 Version Updates

Advisories may be sent to alert customers of significant version updates or patches.

- An advisory should contain links to the release notes, location of the sw packages, and advice of whether customers should update to the new version.
- An advisory could relate to end of life (EOL) or end of support (EOS) for specific versions.

3.4 Support Updates

A support update advisory could pertain to internal information on changes to products supported; or important service related procedures or processes. It may also be used in an unlikely event of service outages to inform customers of any remediation actions.

NTT

Together we do great things