Service Description

Extended End of Vulnerability Support

This Service Description is part of the Services Agreement (as defined in the Services Guide) and describes various Services that Cisco will provide to You. Capitalized terms, unless defined in this document, have the meaning in the Services Guide.

1. Summary

Extended End of Vulnerability Support provides You certain security and vulnerability Operating System Software release(s) for operating system Software [versions] that have reached the end of their life cycle, as described in Cisco's End of Life Policy, (currently available at: http://www.cisco.com/en/US/products/products_end-of-life_policy.html) as applicable on the order. You may purchase this Service as early as the End of Vulnerability Security date of the underlying IOS version and for a duration of up to two (2) years past the Last Date of Support of the corresponding Hardware.

The releases described below are limited to critical severity vulnerabilities as defined in the Security Vulnerability Policy (currently available at: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html) which (a) adversely affect Your network service, (b) have been identified by You to Cisco in writing, and (c) subsequently qualified via Cisco's evaluation process during the Services Term.

Extended End of Vulnerability Support excludes, without limitation, any TAC support, Hardware, or other Software support, such as maintenance releases, upgrades, updates and/or engineering specials.

2. Cisco Responsibilities

- Security and vulnerability Services consist of the following:
  - Cisco will assess any new critical security or vulnerability issues that You identify in writing for the applicability to the Software running on the Product platform and to the configuration used in Your deployment. If applicable, Cisco will first attempt to provide a workaround for Your deployment. If there is no workaround, Cisco will attempt to patch the issue and provide a maintenance release based on latest release.
- Cisco will use commercially reasonable efforts to:
  - Provide Extended Security and Vulnerability for the relevant operating system Software running on the applicable Hardware identified by You and validated by Cisco.

- Work with You to isolate and address the issue(s).

3. Customer Responsibilities

- Engage Your Cisco Account Team to obtain a Cisco private drop site for the Software security release(s).
- Maintain active service coverage for all identified Hardware platform(s) throughout the Services Term.
- Implement a migration plan to remove and/or replace the End of Vulnerability Security by the end of the Services Term.
- You may not make any change in hardware platform, configuration, scale, or topology from the current deployment.