Security Enhancements

Security Enhancements

This section lists enhancements introduced to support Cisco Product Security Requirements and the Product Security Baseline (PSB). For more information about Cisco Product Security Requirements, refer to: https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle/sdl-process.html

PSB Requirements for 21.1.0 Release

Feature Summary and Revision History

Table 1: Summary Data

Applicable Product(s) or Functional Area	CPS/vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 2: Revision History

Revision Details	Release
First introduced	21.1.0

Feature Description

CPS PCRF meets the Cisco security guidelines and is aligned with the security features for 21.1.0 release. CPS now supports the following PSB requirements:

Table 3: CPS PSB Requirements

PSB Item	Description
CT1942: SEC-ASU-SCAN-3	Evaluate the attack surface of an operational offering using automated scanning tools.
CT1933: SEC-OFF-DEFT-4	Disable non-essential services by default.
CT1902: SEC-RUN-ASLR-3	Randomize program address space layout.
CT1884: SEC-RUN-XSPACE-3	Mutually exclude segment write and execute.
CT1940: SEC-VAL-INLDAP	Prevent LDAP injection flows in applications.
CT1935: SEC-WEB-ID-4	Use secure Session Tokens (session IDs/state tokens).
CT1893: SEC-WEB-XSS-3	Prevent cross-site scripting vulnerabilities.
CT1937: SEC-SCR-CONFLEAK-3	Do not expose critical data.
CT1903: SEC-AUT-DEFROOT-2	Do not include non-essential authentication roots.
CT1892: SEC-CRY-PRIM-5	Use approved cryptographic primitives and parameters.
CT1930: SEC-CRY-RANDOM-3	Use approved, well seeded random number generation.
CT1901: SEC-CRE-NOBACK-2	Do not permit undocumented ways of gaining access to the offering.
CT1886: SEC-LOG-NOSENS-3	Do not log sensitive data, passwords, credentials, crypto keys, and so on.
CT1934: SEC-AUT-ANCHOR-2	Anchor authentication trust chains.
CT1140: SEC-CRY-LOG	Log cryptographic connection setup and teardown.
CT1723: SEC-HRD-OS	Harden production components.
CT1741: SEC-PRV-DSRIGHTS	Rights of Personally Identifiable Information's Data Subject.
CT1814: SEC-PWD-CONFIG	Provide configuration options for customer password complexity policy.
CT1929: SEC-LOG-CHANGES	Log system and configuration changes.

CPS vDRA meets the Cisco security guidelines and is aligned with the security features for 21.1.0 release. vDRA now supports the following PSB requirements:

Table 4: CPS vDRA Requirements

PSB Item	Description
CT1942: SEC-ASU-SCAN-3	Evaluate the attack surface of an operational offering using automated scanning tools.

PSB Item	Description
CT1934: SEC-AUT-ANCHOR-2	Anchor authentication trust chains.
CT1930: SEC-CRY-RANDOM-3	Use approved, well seeded random number generation.
CT1933: SEC-OFF-DEFT-4	Disable non-essential services by default.
CT1937: SEC-SCR-CONFLEAK-3	Do not expose critical data.
CT1940: SEC-VAL-INLDAP	Prevent LDAP Injection flows in applications.
CT1935: SEC-WEB-ID-4	Use secure Session Tokens (session IDs/state tokens).
CT1943: SEC-AUT-AUTH-5	Authenticate and authorize remote agents seeking access.
CT1945: SEC-UPS-NOBACK-2	Protect against Supplier backdoors, malware, or known vulnerabilities.
CT672: SEC-DOC-PLATSRV	List needed user platform TCP/IP services.
CT1929: SEC-LOG-CHANGES	Log system and configuration changes.
CT1815: SEC-OUT-CRED-3	No fixed or forced null outbound credentials.
CT578: SEC-DSP-PROC	Display the active TCP/IP services (including open ports).
CT602: SEC-OFF-PROC	Selectively enable TCP/IP SERVICEs/OPEN PORTS.