Security fixes

Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release

This section provides a brief description of the security fixes.

Defect ID - CSCwm98102

The Cisco products UCS B-Series Blade Servers, UCS C-Series Rack Servers and UCS X-Series Compute Nodes may include an optional Trusted Platform Module (TPM) 2.0 that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

- **CVE-2025-2884** — TCG TPM2.0 Reference implementation's CryptHmacSign helper function is vulnerable to Out-of-Bounds read due to the lack of validation the signature scheme with the signature key's algorithm. See Errata Revision 1.83 and advisory TCGVRT0009 for TCG standard TPM2.0.

  Cisco UCS servers equipped with one of the following optional TPM modules:

  - UCSX-TPM2-002
  - UCSX-TPM-002C
  - UCS-TPM-002D
  - UCSX-TPM-002D

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.