

# How does Triple DEA (TDEA) impact ASV Scan results?

PCI SSC FAQ | Article 1452 | September 2017

---

Triple DEA (Data Encryption Algorithm)'also referred to as TDEA, TDES or 3DES'is a cryptographic cipher used in TLS, SSH, IPsec and other protocols and products. TDEA is susceptible to a known vulnerability that is currently ranked as Medium severity by the Common Vulnerability Scoring System (CVSS). As defined in PCI DSS Requirement 11.2.2, vulnerabilities ranked as Medium or High risk by the CVSS must be corrected and the affected systems re-scanned after the corrections to show the issue has been addressed.

ASVs are permitted to re-rank a vulnerability's risk assignment if they disagree with the CVSS (see ASV Program Guide section 6.3.3 'Exceptions to Scoring Vulnerabilities with the NVD'), or if they are able to confirm that the risk level is lower in a particular environment. When making this type of adjustment to the scan report, the ASV should consider the scan customer's unique environment, systems, and controls, and not make adjustments based on general trends or assumptions.

Scan customers are also permitted to dispute the scan findings if they determine a vulnerability was incorrectly reported or if compensating controls or environment-specific factors exist that reduce or eliminate the risk. Refer to ASV Program Guide sections 7.7 "Managing False Positives and Other Disputes" and 7.8 "Addressing Vulnerabilities with Compensating Controls" for details. In all cases, scan customers and ASVs should work together to determine the level of risk that a particular vulnerability may present in a specific environment or configuration.

TDEA has been superseded by the Advanced Encryption Algorithm (AES). Entities using TDEA are encouraged to review their implementations to determine the potential risk that TDEA may present to their environments, and consider transitioning toward a more secure alternative.

Source: <https://www.pcisecuritystandards.org/faqs/1452/>