फ़ाइल संख्या: NCCS/SC/3-1/2025-26
भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग
राष्ट्रीय संचार सुरक्षा केंद्र
https://nccs.gov.in/

दिनांक: 11.03 .2026

अधिसूचना

विषय: सुरक्षा प्रमाणन हेतु उपकरणों का हार्डनिंग – संबंधित ।

उपरोक्त विषय के संबंध में उपकरणों के सुरक्षा परीक्षण एवं प्रमाणन के लिए हार्डनिंग (दृढ़ीकरण) के संबंध में निम्नलिखित निर्देश प्रेषित किए जाते हैं:

1. आवेदक/ओईएम (OEM) परीक्षण प्रारम्भ होने से पूर्व ITSAR-विशिष्ट हार्डनिंग गाइड TSTL को उपलब्ध कराएगा। हार्डनिंग गाइड का एक नमूना प्रारूप परिशिष्ट (Annexure) के रूप में संलग्न है।
2. हार्डनिंग गाइड उपयोगकर्ता के लिए सलाह (Advisories) के रूप में नहीं होना चाहिए। इसमें केवल वे कमांड और चरण शामिल होने चाहिए जो कॉन्फ़िगरेशन के माध्यम से डिवाइस को हार्डन करने के लिए आवश्यक हैं।
3. हार्डनिंग रिबूट के बाद भी प्रभावी (Persist) रहनी चाहिए।
4. गाइड में दी गई पूरी हार्डनिंग प्रक्रिया को TSTL द्वारा DuT पर परीक्षण प्रारम्भ करने से पहले लागू किया जाएगा।
5. सुरक्षा परीक्षण OEM द्वारा प्रदान किए गए हार्डनिंग गाइड के अनुसार पूर्णतः हार्डन किए गए डिवाइस पर किया जाएगा।
6. परीक्षण रिपोर्ट में प्रत्येक ITSAR क्लॉज के लिए TSTL द्वारा स्पष्ट रूप से उल्लेख किया जाएगा कि डिवाइस ITSAR क्लॉज का अनुपालन लागू की गई हार्डनिंग के कारण करता है या डिफ़ॉल्ट स्थिति में ही करता है।
7. मूल्यांकनकर्ता (Evaluator) भी NCCS पोर्टल पर अपलोड की जाने वाली परीक्षण रिपोर्ट में इसी बात को दर्ज करेगा। पोर्टल में 'Complied with Hardening' दर्ज करने के लिए एक फीचर उपलब्ध कराया जाएगा।
8. हार्डनिंग गाइड में आवेदक द्वारा किए गए किसी भी संशोधन का परीक्षण TSTL द्वारा किया जाएगा। हार्डनिंग गाइड का अंतिम संस्करण प्रमाणन से पहले TSTL द्वारा NCCS को प्रस्तुत किया जाएगा। इसके अतिरिक्त, आवेदक अंतिम डिजिटल रूप से हस्ताक्षरित (digitally signed) हार्डनिंग गाइड के सार्वजनिक लिंक को भी प्रदान करेगा, जिसका संदर्भ जारी किए जाने वाले प्रमाणपत्र में दिया जाएगा।

यह आदेश वरिष्ठ उप महानिदेशक, राष्ट्रीय संचार सुरक्षा केंद्र की स्वीकृति से जारी किया गया है।

संलग्न: अनुलग्नक (अंग्रेजी संस्करण में उपलब्ध है।)

हस्ताक्षरित/-

(सुमित सिंह)
सहायक महानिदेशक (सुरक्षा प्रमाणीकरण-I)

सेवा में :
सभी OEMs / डीलर्स / आयातक / आवेदक / TSTLs – NCCS वेबसाइट के माध्यम से

सूचनार्थ प्रतिलिपि:

1. सदस्य (सेवाएँ), डिजिटल संचार आयोग
2. वरिष्ठ उप महानिदेशक, राष्ट्रीय संचार सुरक्षा केंद्र
3. वरिष्ठ उप महानिदेशक, दूरसंचार अभियांत्रिकी केंद्र
4. उप महानिदेशक (सुरक्षा आश्वासन), दूरसंचार विभाग मुख्यालय
5. उप महानिदेशक (दूरसंचार प्रमाणन), दूरसंचार अभियांत्रिकी केंद्र
6. eTT तथा CDoT – पोर्टल में आवश्यक परिवर्तन करने के अनुरोध सहित

File No. NCCS/SC/3-1/2025-26
भारत सरकार/ Government of India
संचार मंत्रालय/Ministry of Communications
दूरसंचार विभाग/Department of Telecommunications
राष्ट्रीय संचार सुरक्षा केंद्र / National Centre for Communication Security
https://nccs.gov.in/

Dated: 11.03.2026

NOTIFICATION

Subject: Hardening of Devices for Security Certification – Reg.

The undersigned is directed to convey the following regarding the hardening of devices for security testing and certification:

1. The Applicant/OEM will provide ITSAR specific hardening guide to the TSTL before the start of testing. A sample format of hardening guide is enclosed as Annexure.
2. The hardening guide shall not be in form of advisories to the user. It should contain only the commands and steps required to harden the device by way of configuration.
3. The hardening shall persist on reboot.
4. The entire hardening procedure as given in the guide shall be applied by the TSTL before commencing the testing on the DuT.
5. The security testing shall be performed on the fully hardened device as per the hardening guide provided by the OEM.
6. In test report for each ITSAR clause, it shall be clearly specified by the TSTL that whether the device complies with the ITSAR clause due to the applied hardening or in the default condition itself.
7. The Evaluator will also record the same in the test report uploaded to NCCS portal. The feature in the portal for recording 'Complied with Hardening' will be made available.
8. Any modifications made by the applicant to the hardening guide shall be tested by the TSTL. The final version of the hardening guide shall be submitted by the TSTL to NCCS prior to certification. Additionally, the applicant shall provide a public link to the final digitally signed version of the hardening guide which will be referenced in the issued certificate.

This is issued with the approval of Sr. DDG, NCCS.

Encl: Annexure

Digitally signed by
SUMIT SINGH
Date: 11-03-2026
17:13:59

(Sumit Singh)
ADG (Security Certification-I)

To,

All OEMs/Dealers/Importers/applicants/TSTLs- through NCCS website

Copy for kind information to:

1. Member(S), DCC
2. Sr. DDG, NCCS
3. Sr. DDG, TEC
4. DDG(SA), DoT HQ
5. DDG(TC), TEC
6. eTT and CDoT – with a request to make necessary changes in the portal

Annexure

Hardening Guide

Cover Page

The cover page design may be as per the choice of the OEM. NCCS/DoT logos or emblem should not be used by the OEM.

In the next page the following information may be captured.

Name and Address of the applicant entity:
Product Name:
Product Variant Name:
ITSAR Ref:
Brand Name:
Model Number:
Model Name:
Portal Application ID:
Main Model:
Associated Model(s):
TSTL:

Table of Contents

The table of contents may be provided for the document.

Preface/Introduction

This section may be provided to explain how to use this hardening guide.

The entire hardening procedure as given in this guide shall be applied by the TSTL before commencing the testing on the DuT.

ITSAR Clause-wise Hardening

This chapter will contain all the clauses for which hardening is to be performed.

Clause 1.1.1 Management Protocols Mutual Authentication

Requirement:

The protocols used for the Network Product's management shall support mutual authentication mechanisms. There is mutual authentication of entities for management interfaces on the network product. HTTPS with TLS 1.2, SNMP V3 Protocols are allowed

Configuration

The following protocols not supporting mutual authentication can be disabled using the following commands:

Protocol1

#command1
#command2

Protocol2

#command1
#command2

…

Clause 1.6.1 Cryptographic Based Secure Communication

Secure communication mechanism between the Network product and the connected entities shall use only the industry standard and NIST recommended cryptographic protocols such as IPSEC, VPN, SSH, TLS/SSL, etc. Also, Network product shall provide all cryptographic service such as encryption, decryption, key exchange, authentication, data integrity etc. using the industry accepted and NIST recommended cryptographic algorithms (with standard key lengths) such as SHA, Diffie-Hellman, AES, RSA etc.

Configuration

The following weaker cryptographic algorithms and ciphers can be disabled using the following commands:

Algo1

#command1
#command2

Algo2

#command1
#command2
……

…….

Similarly, for all other ITSAR clauses for which the OEM intends to provide Hardening are to be mentioned here by adding sections as shown above for the two clauses.

Glossary

If necessary

References

If necessary