Guide to the Secure Configuration of Fedora

with profile OSPP - Protection Profile for General Purpose Operating Systems

— This profile reflects mandatory configuration controls identified in the NIAP Configuration Annex to the Protection Profile for General Purpose Operating Systems (Protection Profile Version 4.2).

As Fedora OS is moving target, this profile does not guarantee to provide security levels required from US National Security Systems. Main goal of the profile is to provide Fedora developers with hardened environment similar to the one mandated by US National Security Systems.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide

This guide presents a catalog of security-relevant configuration settings for Fedora. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Evaluation target	Inanna.
Benchmark URL	#scap_org.open-scap_comp_ssg-fedora-xccdf.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_FEDORA
Benchmark version	0.1.75
Profile ID	xccdf_org.ssgproject.content_profile_ospp
Started at	2025-05-26T18:52:43-06:00
Finished at	2025-05-26T18:53:51-06:00

Performed by	root
Test system	cpe:/a:redhat:openscap:1.4.2

CPE Platforms

- **cpe:/o:fedoraproject:fedora:39**
- **cpe:/o:fedoraproject:fedora:40**
- **cpe:/o:fedoraproject:fedora:41**
- **cpe:/o:fedoraproject:fedora:42**
- **cpe:/o:fedoraproject:fedora:43**
- **cpe:/o:fedoraproject:fedora:44**
- **cpe:/o:fedoraproject:fedora:45**

Addresses

- **IPv4** 127.0.0.1
- **IPv4** 10.255.255.254
- **IPv4** 172.19.81.111
- **IPv6** 0:0:0:0:0:0:0:1
- **IPv6** fe80:0:0:0:215:5dff:fedc:bfe5
- **MAC** 00:00:00:00:00:00
- **MAC** 00:15:5D:DC:BF:E5

Compliance and Scoring

The target system did not satisfy the conditions of 22 rules! Please review rule results and consider applying remediation.

Rule results

8 passed

22 failed

0 other

Severity of failed rules

0 other

1 low

18 medium

3 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	56.388889	100.000000	56.39%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Fedora **22x fail**		
System Settings **22x fail**		
Installing and Maintaining Software **7x fail**		
System and Software Integrity **2x fail**		
Software Integrity Checking		
Federal Information Processing Standard (FIPS)		
System Cryptographic Policies **1x fail**		
Configure BIND to use System Crypto Policy	high	**notapplicable**
Configure System Cryptography Policy	high	**fail**
Configure Kerberos to use System Crypto Policy	high	**pass**
Configure Libreswan to use System Crypto Policy	high	**pass**
Configure OpenSSL library to use System Crypto Policy	medium	**pass**
Configure SSH to use System Crypto Policy	medium	**pass**
Operating System Vendor Support and Certification **1x fail**		
The Installed Operating System Is Vendor Supported	high	**fail**
GNOME Desktop Environment		
System Tooling / Utilities		
Updating Software **5x fail**		
Install dnf-automatic Package	medium	**fail**
Configure dnf-automatic to Install Available Updates Automatically	medium	**fail**
Configure dnf-automatic to Install Only Security Updates	low	**fail**
Ensure Fedora GPG Key Installed	high	**fail**
Ensure gpgcheck Enabled In Main dnf Configuration	high	**notapplicable**
Ensure gpgcheck Enabled for Local Packages	high	**notapplicable**
Ensure gpgcheck Enabled for All dnf Package Repositories	high	**pass**
Enable dnf-automatic Timer	medium	**fail**
Account and Access Control **10x fail**		
Warning Banners for System Accesses		

Title	Severity	Result
Protect Accounts by Configuring PAM **10x fail**		
Set Lockouts for Failed Password Attempts **4x fail**		
Lock Accounts After Failed Password Attempts	medium	**fail**
Configure the root Account for Failed Password Attempts	medium	**fail**
Set Interval For Counting Failed Password Attempts	medium	**fail**
Set Lockout Time for Failed Password Attempts	medium	**fail**
Set Password Quality Requirements **6x fail**		
Set Password Quality Requirements with pam_pwquality **6x fail**		
Ensure PAM Enforces Password Requirements - Minimum Digit Characters	medium	**fail**
Ensure PAM Enforces Password Requirements - Minimum Lowercase Characters	medium	**fail**
Ensure PAM Enforces Password Requirements - Minimum Length	medium	**fail**
Ensure PAM Enforces Password Requirements - Minimum Special Characters	medium	**fail**
Ensure PAM Enforces Password Requirements - Authentication Retry Prompts Permitted Per-Session	medium	**fail**
Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters	medium	**fail**
Protect Physical Console Access		
Protect Accounts by Restricting Password-Based Login		
Secure Session Configuration Files for Login Accounts		
GRUB2 bootloader configuration		
Configure Syslog		
Network Configuration and Firewalls		
File Permissions and Masks **5x fail**		
Restrict Partition Mount Options **3x fail**		
Add nodev Option to /dev/shm	medium	**fail**
Add noexec Option to /dev/shm	medium	**fail**
Add nosuid Option to /dev/shm	medium	**fail**
Restrict Programs from Dangerous Execution Patterns **2x fail**		

Title	Severity	Result
Disable Core Dumps **2x fail**		
Disable acquiring, saving, and processing core dumps	medium	**notapplicable**
Disable core dump backtraces	medium	**fail**
Disable storing core dump	medium	**fail**
Enable ExecShield		
Memory Poisoning		
Disable storing core dumps	medium	**notapplicable**
Restrict Access to Kernel Message Buffer	low	**notapplicable**
Disable Kernel Image Loading	medium	**notapplicable**
Disallow kernel profiling by unprivileged users	low	**notapplicable**
Disable Access to Network bpf() Syscall From Unprivileged Processes	medium	**notapplicable**
Restrict usage of ptrace to descendant processes	medium	**notapplicable**
Harden the operation of the BPF just-in-time compiler	medium	**notapplicable**
Disable the use of user namespaces	medium	**notapplicable**
SELinux		
Services		
System Accounting with auditd		

Generated using OpenSCAP 1.4.2