Product Security

CentOS Security Enhancements/Kernel Upgrade

Feature Summary and Revision History

Table 1: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Not Applicable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 2: Revision History

Revision Details	Release
CentOS upgraded to 8.1 Kernel upgraded to 4.18.0-147.5.1.el8_1 Grafana upgraded to 6.7.1-1	20.2.0
Kernel upgraded to 3.10.0-957.12.2.el7 Grafana upgraded to 6.2.2-1	19.4.0
CentOS upgraded to 7.6 (1810) Kernel upgraded to 3.10.0-957.10.1.el7	19.3.0
Kernel upgraded to 3.10.0-957.5.1.el7	19.2.0
Kernel upgraded to 3.10.0-957.e17	19.1.0

Revision Details	Release
First introduced: kernel upgraded to 3.10.0-862.14.4.el7.x86_64	18.5.0

Feature Description

In this release, the following upgrades have been done to fix the vulnerabilities:

- CentOS upgraded from 7.6 to 8.1
- Kernel upgraded from 3.10.0-957.12.2.el7 to 4.18.0-147.5.1.el8_1
- Grafana upgraded from 6.2.2-1 to 6.7.1-1

For service-related issues, you can use `journactl` to get systemctl logs.