

COMPLIANCE REPORT: CJIS v5.9.3

Summary

Controls Passed	00
Controls Needs Attention	02
Missed Check-Ins	01

SI-System and Information Integrity

SI-2 Flaw Remediation

Status: **Needs Attention**

58 Vulnerable Assets

12 Missed Check-Ins

Requirement:

The organization:

- Identifies, reports, and corrects information system flaws;
- Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
- Incorporates flaw remediation into the organizational configuration management process.

Outdated Assets (16):

desktop-e1evk1g	lenovop361tiny	desktop-e1evk1g	lenovop361tiny
desktop-5njtlrc	desktop-e1evk1g	desktop-5njtlrc	desktop-e1evk1g
optiplex3040	desktop-5njtlrc	optiplex3040	desktop-5njtlrc
lenovop360tiny	optiplex3040	lenovop360tiny	optiplex3040

Missed Check-Ins (16):

desktop-e1evk1g	optiplex3040	lenovop361tiny	desktop-5njtlrc
desktop-5njtlrc	lenovop360tiny	desktop-e1evk1g	optiplex3040

desktop-e1evk1g	optiplex3040	lenovop361tiny	desktop-5njtlrc
desktop-5njtlrc	lenovop360tiny	desktop-e1evk1g	optiplex3040

Vulnerabilities (17):

1. Flash Descriptor Unlocked (High - 7.5) (16 Assets)

desktop-e1evk1g	lenovop361tiny	desktop-e1evk1g	lenovop361tiny
desktop-5njtlrc	desktop-e1evk1g	desktop-5njtlrc	desktop-e1evk1g
optiplex3040	desktop-5njtlrc	optiplex3040	desktop-5njtlrc
lenovop360tiny	optiplex3040	lenovop360tiny	optiplex3040

2. Insecure Flash Access Control (High - 7.5) (12 Assets)

desktop-e1evk1g	desktop-e1evk1g	desktop-e1evk1g	lenovop361tiny
desktop-5njtlrc	desktop-5njtlrc	optiplex3040	desktop-5njtlrc
optiplex3040	optiplex3040	lenovop360tiny	optiplex3040

3. Microarchitectural Data Sampling (High - 7.5) (32 Assets)

desktop-e1evk1g	lenovop361tiny	desktop-e1evk1g	lenovop361tiny
desktop-5njtlrc	desktop-e1evk1g	desktop-5njtlrc	desktop-e1evk1g
optiplex3040	desktop-5njtlrc	optiplex3040	desktop-5njtlrc
lenovop360tiny	optiplex3040	lenovop360tiny	optiplex3040
desktop-e1evk1g	desktop-e1evk1g	desktop-e1evk1g	desktop-e1evk1g
desktop-5njtlrc	desktop-5njtlrc	desktop-5njtlrc	desktop-5njtlrc
optiplex3040	optiplex3040	optiplex3040	optiplex3040
lenovop360tiny	lenovop360tiny	lenovop360tiny	lenovop360tiny

4. Outdated Microcode (Medium - 5.5) (58 Assets)

desktop-e1evk1g	optiplex3040	lenovop360tiny	optiplex3040
desktop-5njtlrc	lenovop360tiny	desktop-e1evk1g	lenovop360tiny
optiplex3040	desktop-e1evk1g	desktop-5njtlrc	optiplex3040
lenovop360tiny	lenovop361tiny	optiplex3040	lenovop360tiny
desktop-e1evk1g	desktop-e1evk1g	lenovop360tiny	desktop-e1evk1g
desktop-5njtlrc	desktop-5njtlrc	desktop-5njtlrc	desktop-5njtlrc
optiplex3040	optiplex3040	desktop-e1evk1g	optiplex3040
lenovop360tiny	desktop-e1evk1g	desktop-5njtlrc	lenovop360tiny
optiplex3040	desktop-5njtlrc	optiplex3040	lenovop361tiny
lenovop360tiny	optiplex3040	lenovop360tiny	desktop-e1evk1g
desktop-e1evk1g	lenovop360tiny	desktop-e1evk1g	desktop-5njtlrc
desktop-5njtlrc	optiplex3040	desktop-5njtlrc	optiplex3040

desktop-e1evk1g	lenovop360tiny	desktop-e1evk1g	lenovop360tiny
desktop-5njtlrc	optiplex3040	desktop-5njtlrc	
optiplex3040	lenovop360tiny	optiplex3040	

5. Spectre 2: Branch Target Injection (Medium - 5.5) (7 Assets)

desktop-e1evk1g	optiplex3040	desktop-e1evk1g	lenovop360tiny
desktop-5njtlrc	lenovop360tiny	desktop-5njtlrc	

6. Spectre 4: Speculative Store Bypass (Medium - 5.5) (5 Assets)

desktop-e1evk1g	optiplex3040	desktop-e1evk1g	lenovop360tiny
desktop-5njtlrc			

7. Spectre 3a: Rogue System Register Read (Medium - 5.5) (5 Assets)

desktop-e1evk1g	optiplex3040	desktop-e1evk1g	lenovop360tiny
desktop-5njtlrc			

8. Spectre (OS Misconfiguration) (Medium - 5.5) (5 Assets)

desktop-e1evk1g	optiplex3040	desktop-e1evk1g	lenovop360tiny
desktop-5njtlrc			

9. Foreshadow (Medium - 5.5) (5 Assets)

desktop-e1evk1g	optiplex3040	desktop-e1evk1g	lenovop360tiny
desktop-5njtlrc			

10. Intel ME Remote Privilege Escalation (Low - 2.2) (5 Assets)

desktop-e1evk1g	optiplex3040	desktop-e1evk1g	lenovop360tiny
desktop-5njtlrc			

11. Meltdown (Low - 2.2) (2 Assets)

optiplex3040	lenovop360tiny
------------------------------	--------------------------------

12. SMI Unlocked (Low - 2.2) (7 Assets)

desktop-e1evk1g	optiplex3040	desktop-e1evk1g	desktop-5njt3rc
desktop-5njtlrc	lenovop360tiny	desktop-5njtlrc	

13. ROCA (Low - 2.2) (6 Assets)

[desktop-e1evk1g](#) [optiplex3040](#) [desktop-5njtlrc](#) [desktop-5njt3rc](#)
[desktop-5njtlrc](#) [lenovop360tiny](#)

14. DCI Debug Enabled (CVE-2017-5684) (Low - 2.2) (8 Assets)

[desktop-e1evk1g](#) [optiplex3040](#) [desktop-e1evk1g](#) [desktop-5njtlrc](#)
[desktop-5njtlrc](#) [lenovop360tiny](#) [desktop-5njtlrc](#) [desktop-5njt3rc](#)

15. Processor Memory Unlocked (Low - 2.2) (1 Asset)

[desktop-e1evk1g](#)

16. Pantsdown (CVE-2019-6260). Aspeed BMC iLPC2AHB Bridge Misconfiguration (Low - 2.2) (5 Assets)

[desktop-e1evk1g](#) [optiplex3040](#) [desktop-e1evk1g](#) [desktop-5njt3rc](#)
[desktop-5njtlrc](#)

17. Pantsdown (CVE-2019-6260). Aspeed BMC P2A Bridge Misconfiguration (Low - 2.2) (5 Assets)

[desktop-e1evk1g](#) [optiplex3040](#) [desktop-e1evk1g](#) [desktop-5njt3rc](#)
[desktop-5njtlrc](#)

SI-4 Information System Monitoring

Status: Missed Check-in

70 Missed Check-Ins

Requirement:

The organization:

- e. Monitors the information system to detect:
 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and
 2. Unauthorized local, network, and remote connections;
- b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
- c. Deploys monitoring devices:
 1. Strategically within the information system to collect organization-determined essential information; and
 2. At ad hoc locations within the system to track specific types of transactions of interest to the

organization;

- d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
- f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
- g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

Missed Check-Ins (12):

[desktop-e1evk1g](#)

[lenovop361tiny](#)

[desktop-e1evk1g](#)

[lenovop361tiny](#)

[desktop-5njtlrc](#)

[desktop-e1evk1g](#)

[desktop-5njtlrc](#)

[desktop-e1evk1g](#)

[optiplex3040](#)

[desktop-5njtlrc](#)

[optiplex3040](#)

[desktop-5njtlrc](#)

SI-7 Software, Firmware, and Information Integrity

Status: **Need Attention**

70 Integrity Failures

Requirement:

- a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and
- b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].

Integrity Failures (30):

[desktop-e1evk1g](#)

[optiplex3040](#)

[desktop-e1evk1g](#)

[lenovop360tiny](#)

[desktop-5njtlrc](#)

[lenovop360tiny](#)

[desktop-5njtlrc](#)

[desktop-](#)

[optiplex3040](#)

[desktop-e1evk1g](#)

[optiplex3040](#)

[lenovop360tiny](#)

[lenovop360tiny](#)

[desktop-5njtlrc](#)

[desktop-e1evk1g](#)

[desktop-e1evk1g](#)

[desktop-e1evk1g](#)

[optiplex3040](#)

[desktop-5njtlrc](#)

[desktop-5njtlrc](#)

[desktop-5njtlrc](#)

[lenovop360tiny](#)

[optiplex3040](#)

[optiplex3040](#)

[optiplex3040](#)

[desktop-e1evk1g](#)

[lenovop360tiny](#)

[lenovop361tiny](#)

[lenovop360tiny](#)

[lenovop361tiny](#)

Appendix: Vulnerabilities

Flash Descriptor Unlocked

Severity: Critical - 9.5

Overview:

Flash Descriptor write-protection protects settings on the Flash from being maliciously or unintentionally changed after manufacturing is completed.

Description:

If the equipment manufacturer doesn't enable Intel-recommended Flash Descriptor write protections, a privileged, local attacker can modify the contents of the Flash Descriptor region. This allows an attacker to change access permissions for other regions or change layout for any regions which may be used to bypass hardware protections like PR registers and BIOS Control Register.

Recommendation:

Potential Firmware Update: Fixes are available for certain platforms from certain vendors. Check latest firmware in vendor web-site and install the latest updates.

Additional Information:

- https://github.com/abazhaniuk/Publications/blob/master/2017/44CON_2017/Bulygin_Bazhaniuk_44con.pdf

Assets Affected (16):

desktop-e1evk1g	lenovop361tiny	desktop-e1evk1g	lenovop361tiny
desktop-5njtlrc	desktop-e1evk1g	desktop-5njtlrc	desktop-e1evk1g
optiplex3040	desktop-5njtlrc	optiplex3040	desktop-5njtlrc
lenovop360tiny	optiplex3040	lenovop360tiny	optiplex3040