CVE-2026-20709

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-20709
State	PUBLISHED
Assigner	intel
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 19:25:12 UTC
Updated	2026-04-08 21:26:13 UTC
Description	Use of Default Cryptographic Key in the hardware for some Intel(R) Pentium(R) Processor Silver Series, Intel(R) Celeron(R

Risk And Classification

Primary CVSS: v4.0 5.8 MEDIUM from secure@intel.com

CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000170000 probability, percentile 0.041180000 (date 2026-04-14)

Problem Types: CWE-1394 | Escalation of Privilege | CWE-1394 Use of Default Cryptographic Key

Version	Source	Type	Score	Severity	Vector
4.0	secure@intel.com	Secondary	5.8	MEDIUM	CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:N/E:X/C
4.0	CNA	CVSS	5.8	MEDIUM	CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:N
3.1	secure@intel.com	Secondary	6.6	MEDIUM	CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N
3.1	CNA	CVSS	6.6	MEDIUM	CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product
CNA	Na	IntelR PentiumR Processor Silver Series IntelR CeleronR Processor J Series IntelR CeleronR Processor N Series May Al

References

Reference	Source	Link	Tags
intel.com/content/www/us/en/security-center/advisory/intel-sa-00609.html	secure@intel.com	intel.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.