



CVE-2026-4272 - Bluetooth Remote Execution of System Commands Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-4272
State	PUBLISHED
Assigner	Honeywell
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-05 22:16:01 UTC
Updated	2026-04-07 13:20:35 UTC

Description Missing Authentication for Critical Function vulnerability in Honeywell Handheld Scanners allows Authentication Abuse.This

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from psirt@honeywell.com

CVSS: 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

EPSS: 0.001090000 probability, percentile 0.291690000 (date 2026-04-07)

Problem Types: CWE-306 | CWE-306 CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
3.1	psirt@honeywell.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Honeywell	Barcode Scanners	affected C1 Base(Ingenic x1000) GK000432BAA custom	Not speci
CNA	Honeywell	Barcode Scanners	affected D1 Base(Ingenic x1600) HE000085BAA custom	Not speci
CNA	Honeywell	Barcode Scanners	affected A1/B1 Base(IMX25) BK000763BAA_BK000765BAA_CU000101BAA custom	Not speci

References

Reference	Source	Link	Tags
https://nvd.nist.gov/vuln/detail/CVE-2026-4272	psirt@honeywell.com	https	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Kaspersky (en)

CNA: Haidar Kabibo (en)

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report