ADVANTECH Enabling an Intelligent Planet

No. 1, Alley 20, Lane 26, Rueiguang Road,
Neihu District, Taipei 11491, Taiwan, R.O.C.
Tel: 886-2-2792-7818
Fax: 886-2-2218-3650

Vulnerabilities Identified in EKI-6333AC-2G/EKI-6333AC-2GD/EKI-6333AC-1GPO

Version: V1.1

Release Date: Nov 25, 2024

We announce the release of a new firmware update of EKI-6333AC-2G, EKI-6333AC-2GD, EKI-6333AC-1GPO, that addresses several vulnerabilities identified in our system. This update is part of our ongoing commitment to maintaining the highest security standards and ensuring the safety of our users' data and operations

Reason of Product Change

In previous firmware versions of the EKI-6333AC-2G, EKI-6333AC-2GD, and EKI-6333AC-1GPO, several vulnerabilities were identified. Following a thorough triage and confirmation of these issues, Advantech has released updated firmware to address them, with approval from Nozomi Networks Labs. Firmware version 1.6.5 is now available for the EKI-6333AC-2G and EKI-6333AC-2GD, while firmware version 1.2.2 has been released for the EKI-6333AC-1GPO.

Vulnerability Scoring Details

Item	CVE ID	CWE	CVSS v3.1 Base Score	CVSS v3.1 Vector
1	CVE-2024-50370, CVE-2024-50371, CVE-2024-50372, CVE-2024-50373, CVE-2024-50374,	Improper Neutralization of Special Elements used in an OS Command (CWE-78)	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2	CVE-2024-50359, CVE-2024-50360, CVE-2024-50361, CVE-2024-50362, CVE-2024-50363, CVE-2024-50364, CVE-2024-50365, CVE-2024-50366, CVE-2024-50367, CVE-2024-50368, CVE-2024-50369	Improper Neutralization of Special Elements used in an OS Command (CWE-78)	7.2	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3	CVE-2024-50375	Missing Authentication for Critical Function (CWE-306)	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
4	CVE-2024-50376	Improper Neutralization of Input During Web Page Generation ('Cross-Site Scripting') (CWE-79)	7.3	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H
5	CVE-2024-50358	External Control of System or Configuration Setting (CWE-15)	7.2	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
6	CVE-2024-50377	Use of Hard-coded Credentials (CWE-798)	6.5	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H

Affected Products

We strongly recommend all users update their devices to this latest firmware version as soon as possible. The update is available for download on our official website

	Vulnerabilities fixed version	Download page
EKI-6333AC-2G	v1.6.5	https://www.advantech.com/en/support/details/firmware?id=1-1Y1Q6G7
EKI-6333AC-2GD		
EKI-6333AC-1GPO	v1.2.2	https://www.advantech.com/en/support/details/firmware?id=1-2NPZ6GU

Advantech