



CVE-2019-7232

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

Summary

CVE	CVE-2019-7232
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-24 17:15:00 UTC
Updated	2022-11-30 21:41:00 UTC
Description	The ABB IDAL HTTP server is vulnerable to a buffer overflow when a long Host header is sent in a web request. The Host I

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Abb	Pb610 Panel Builder 600	-	All	All	All
Hardware	Abb	Pb610 Panel Builder 600	-	All	All	All
Operating System	Abb	Pb610 Panel Builder 600 Firmware	All	All	All	All

References

Reference	Source	Link	Ta
Multiple Vulnerabilities in ABB PB610	CONFIRM	search.abb.com	Mit
Full Disclosure: XL-19-011 - ABB IDAL HTTP Server Stack-Based Buffer Overflow Vulnerability	MISC	seclists.org	Ex
404 Not Found	MISC	www.darkmatter.ae	Th
ABB IDAL HTTP Server Stack-Based Buffer Overflow ≈ Packet Storm	MISC	packetstormsecurity.com	Ex
ABB PB610 Multiple Security Vulnerabilities	BID	www.securityfocus.com	Th
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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](#)