



CVE-2018-1149

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

Summary

CVE	CVE-2018-1149
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-19 15:29:00 UTC
Updated	2018-12-07 19:36:00 UTC
Description	cgi_system in NUUO's NVRMini2 3.8.0 and below allows remote attackers to execute arbitrary code via crafted HTTP requ

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nuuu	Nvrmini2	-	All	All	All
Hardware	Nuuu	Nvrmini2	-	All	All	All
Operating System	Nuuu	Nvrmini2 Firmware	All	All	All	All

References

Reference	Source	Link
poc/nuuu/nvrmini2 at master · tenable/poc · GitHub	CONFIRM	github.com
NUUO NVRmini 2 and NVRsolo Remote Code Execution and Stack Based Buffer Overflow Vulnerabilities	BID	www.securityfocus.com
[R2] Multiple NUUO NVRMini2 Vulnerabilities - Research Advisory Tenable®	MISC	www.tenable.com
www.nuuu.com/backend/CKEdit/upload/files/NUUO_NVRsolo_v3_9_1_Release%20not...	CONFIRM	www.nuuu.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)