



CVE-2022-22986

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

Summary

CVE	CVE-2022-22986
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-31 08:15:00 UTC
Updated	2022-04-08 13:23:00 UTC
Description	Netcommunity OG410X and OG810X series (Netcommunity OG410Xa, OG410Xi, OG810Xa, and OG810Xi firmware Ver.2

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Ntt-east	Og410xa	-	All	All	All
Operating System	Ntt-east	Og410xa Firmware	All	All	All	All
Hardware	Ntt-east	Og410xi	-	All	All	All
Operating System	Ntt-east	Og410xi Firmware	All	All	All	All
Hardware	Ntt-east	Og810xa	-	All	All	All
Operating System	Ntt-east	Og810xa Firmware	All	All	All	All
Hardware	Ntt-east	Og810xi	-	All	All	All
Operating System	Ntt-east	Og810xi Firmware	All	All	All	All

References

Reference

Netcommunity OG410X810Xシリーズをご利用のお客さまへ お知らせ 法人のお客さま NTT東日本
JVNVU#94900322: Netcommunity OG410X and OG810X VoIP gateway/Hikari VoIP adapter for business offices vulnerable to OS command i
【NTT西日本】「Netcommunity OG410X810Xシリーズ」をご利用のお客さまへ - 法人・企業向けICTサービス
CVE Program record
NVD vulnerability detail

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](#)