2024年第12号

サイバーセキュリティの置き薬

Toyama Prefectural Police Cyber Security Personnel

CENTURY SYSTEMS社製品を利用している皆様へ

VPNﾙｰﾀ（FutureNet NXRｼﾘｰｽﾞ・VXRｼﾘｰｽﾞ）及び仮想ｿﾌﾄｳｪｱﾙｰﾀ（WXRｼﾘｰｽﾞ）における脆弱性が公開

(CVE-2024-31070, CVE-2024-36475, CVE-2024-36491及びCVE-2020-10188)

公開された脆弱性が放置されたままだと、攻撃者に悪用され、Telnetに無制限にアクセスされる、外部から任意コマンドを実行される、機微な情報を窃取・改ざんされたりサービス運用妨害攻撃等を受ける可能性があります。

【影響を受けるシステム／バージョン】

○CVE-2024-31070

当該製品を初期設定のまま使用しているもの

○CVE-2024-36475, CVE-2024-34691及びCVE-2020-10188

NXR-1300ｼﾘｰｽﾞ(7.4.9)	NXR-650(21.16.1)	NXR-610Xｼﾘｰｽﾞ(21.14.11)
NXR-530(21.11.13)	NXR-350/C(5.30.9)	NXR-230/C(5.30.12)
NXR-160/LW(21.8.3)	NXR-G200ｼﾘｰｽﾞ(9.12.15)	NXR-G180/L-CA(21.7.28B)
NXR-G120ｼﾘｰｽﾞ(21.15.2)	NXR-G110ｼﾘｰｽﾞ(21.7.30C)	NXR-G100ｼﾘｰｽﾞ(6.23.10)
NXR-G060ｼﾘｰｽﾞ(21.15.5)	NXR-G050ｼﾘｰｽﾞ(21.12.9)	VXR/x64(21.7.31)
VXR/x86(10.1.4)	NXR-1200(5.25.21)	NXR-130/C(5.13.21)
NXR-155/Cｼﾘｰｽﾞ(5.22.5M)	NXR-125/CX(5.25.7H)	NXR-120/C(5.25.7H)
WXR-250(1.4.7)	※( )内以前のバージョンが対象	

【推奨される対策】

○CVE-2024-31070

・CLIコマンドを利用してTelnetを無効化し、SSHを利用

※2024/06/28以降リリースのファームウェアバージョンは、上記設定済み

○CVE-2024-36475, CVE-2024-34691及びCVE-2020-10188

・最新のファームウェアに**アップデート**してください

・サポートが終了した製品は、**使用停止もしくは後続製品へ移行**

【参考情報】

・https://www.centurysys.co.jp/backnumber/nxr_common/20240716-01.html
(ｾﾝﾁｭﾘｰ・ｼｽﾃﾑｽﾞ製FutureNet NXRｼﾘｰｽﾞ、VXRｼﾘｰｽﾞおよびWXRｼﾘｰｽﾞにおける複数の脆弱性について)

・https://jvn.jp/vu/JVNVU96424864/index.html
(JVNVU#96424864 ｾﾝﾁｭﾘｰ・ｼｽﾃﾑｽﾞ製FutureNetNXRｼﾘｰｽ、VXRｼﾘｰｽﾞおよびWXRｼﾘｰｽﾞにおける複数の脆弱性)

被害に遭った場合は、
サイバー犯罪対策課にご連絡を！
連絡先 076-441-2211(代表)

【参考】
「ｻｲﾊﾞｰｾｷｭﾘﾃｨの置き薬」
バックナンバーです。