



CVE-2020-5633

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

Summary

CVE	CVE-2020-5633
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-13 10:15:00 UTC
Updated	2021-01-21 19:00:00 UTC
Description	Multiple NEC products (Express5800/T110j, Express5800/T110j-S, Express5800/T110j (2nd-Gen), Express5800/T110j-S (2nd-Gen)) are vulnerable to a remote denial of service attack via a specially crafted network packet. The attack exploits a buffer overflow in the network stack, causing the system to crash and become unavailable. The vulnerability affects all versions of the affected products.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Nec	Baseboard Management Controller	All	All	All	All
Hardware	Nec	Express5800/gt110j	-	All	All	All
Hardware	Nec	Express5800/gt110j	-	All	All	All
Hardware	Nec	Express5800/t110j	-	All	All	All
Hardware	Nec	Express5800/t110j	-	All	All	All
Hardware	Nec	Express5800/t110j-s	-	All	All	All
Hardware	Nec	Express5800/t110j-s	-	All	All	All
Hardware	Nec	Express5800/t110j-s 2nd-gen	-	All	All	All
Hardware	Nec	Express5800/t110j-s 2nd-gen	-	All	All	All
Hardware	Nec	Express5800/t110j 2nd-gen	-	All	All	All
Hardware	Nec	Express5800/t110j 2nd-gen	-	All	All	All
Hardware	Nec	Istorage Ns100ti	-	All	All	All
Hardware	Nec	Istorage Ns100ti	-	All	All	All

References

Reference	Source	Link	Tags
JVN#38752718: Multiple NEC Products vulnerable to authentication bypass	MISC	jvn.jp	Third Party Advisory

NV21-002: セキュリティ情報 NEC	MISC	jpn.nec.com	Vendor Advisory
修正情報・ダウンロード・詳細: 修正情報・ダウンロード・検索一覧 NEC	MISC	www.support.nec.co.jp	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report