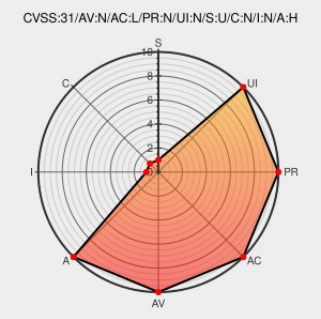
CVE-2021-25306

Published on: 03/01/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:50 PM UTC

CVE-2021-25306

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dx600a from Gigaset contain the following vulnerability:

A buffer overflow vulnerability in the AT command interface of Gigaset DX600A v41.00-175 devices allows remote attackers to force a device reboot by sending relatively long AT commands.

CVE-2021-25306 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Technical Advisory: Administrative Passcode Recovery and Authenticated Remote Buffer Overflow Vulnerabilities in Gigaset DX600A Handset (CVE-2021-25309, CVE-2021-25306) – NCC Group Research	Third Party Advisory research.nccgroup.com text/html	MISC research.nccgroup.com/2021/02/28/technical-advisory-administrative-passcode-recovery-and-authenticated-remote-buffer-overflow-vulnerabilities-in-gigaset-dx600a-handset-cve-

2021-25309-cve-2021-25306/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Gigaset	Dx600a	-	All	All	All
Hardware	Gigaset	Dx600a	-	All	All	All
Hardware	Gigaset	Dx600a	-	All	All	All
Operating System	Gigaset	Dx600a Firmware	v41.00-175	All	All	All
Operating System	Gigaset	Dx600a Firmware	v41.00-175	All	All	All

cpe:2.3:h:gigaset:dx600a:-:*:*:*:*:*:*:*:

cpe:2.3:h:gigaset:dx600a:-:*:*:*:*:*:*:*:

cpe:2.3:h:gigaset:dx600a:-:*:*:*:*:*:*:*:

cpe:2.3:o:gigaset:dx600a_firmware:v41.00-175:*:*:*:*:*:*:*:

cpe:2.3:o:gigaset:dx600a_firmware:v41.00-175:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→