



CVE-2021-25309

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

Last Modified on: 04/26/2022 04:00:00 PM UTC

CVE-2021-25309

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Dx600a](#) from [Gigaset](#) contain the following vulnerability:

The telnet administrator service running on port 650 on Gigaset DX600A v41.00-175 devices does not implement any lockout or throttling functionality. This situation (together with the weak password policy that forces a 4-digit password) allows remote attackers to easily obtain administrative access via brute-force attacks.

CVE-2021-25309 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

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

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

Social Mentions		
Source	Title	Posted (UTC)
 @lofi42	Good old time ... CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H https://t.co/U2yo3EC7gg	2022-04-27 16:04:00

[site](#). This site includes MITRE data granted under the following [license](#).

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