



CVE-2022-41004

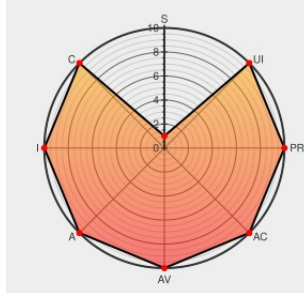
Published on: Not Yet Published

Last Modified on: 02/03/2023 05:10:00 PM UTC

CVE-2022-41004

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Quartz-gold](#) from [Siretta](#) contain the following vulnerability:

Several stack-based buffer overflow vulnerabilities exist in the DetranCLI command parsing functionality of Siretta QUARTZ-GOLD G5.0.1.5-210720-141020. A specially-crafted network packet can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities. This buffer overflow is in the function that manages the 'no ip nat outside source (udp|tcp|all) (WORD|null) WORD to A.B.C.D (WORD|null) description (WORD|null)' command template.

CVE-2022-41004 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Cisco](#) **Siretta** - **QUARTZ-GOLD** version = **G5.0.1.5-210720-141020**

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

CVE References

Description	Tags	Link
TALOS-2022-1613 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1613

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 	Siretta	Quartz-gold	-	All	All	All
Operating System	Siretta	Quartz-gold Firmware	g5.0.1.5-210720-141020	All	All	All
cpe:2.3:h:siretta:quartz-gold:-:*****:.*:						
cpe:2.3:o:siretta:quartz-gold_firmware:g5.0.1.5-210720-141020:*****:.*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	cve.report/CVE-2022-41004 Several stack-based buffer overflow vulnerabilities exist in the DetranCLI command parsing... twitter.com/i/web/status/1...	2023-01-26 23:26:23

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)