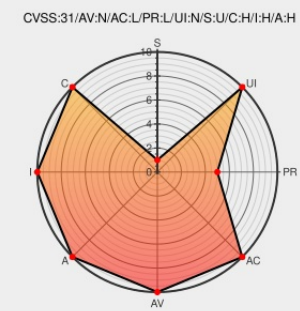
CVE-2022-36279

Published on: Not Yet Published

Last Modified on: 02/02/2023 05:23:00 PM UTC

CVE-2022-36279

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



Certain versions of Quartz-gold from Siretta contain the following vulnerability:

A stack-based buffer overflow vulnerability exists in the httpd delfile.cgi functionality of Siretta QUARTZ-GOLD G5.0.1.5-210720-141020. A specially-crafted HTTP request can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability.

CVE-2022-36279 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Siretta** - **QUARTZ-GOLD** version **= G5.0.1.5-210720-141020**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
TALOS-2022-1605 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1605

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-2022-36279 A stack-based buffer overflow vulnerability exists in the httpd delfile.cgi functionality… twitter.com/i/web/status/1…	2023-01-26 23:16:16

← Previous ID

Next ID→