# CVE Detail – CVE-2022-3203

On ORing net IAP-420(+) with FW version 2.0m a telnet server is enabled by default and cannot permanently be disabled. You can connect to the device via LAN or WiFi with hardcoded credentials and get an administrative shell. These credentials are reset to defaults with every reboot.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.29421

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-912: Hidden Functionality

## CAPEC(s)

* CAPEC-133: Try All Common Switches
* CAPEC-190: Reverse Engineer an Executable to Expose Assumed Hidden Functionality

## Affected Products

* cpe:2.3:o:oringnet:iap-420\+\_firmware:2.0m:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:oringnet:iap-420\_firmware:2.0m:\*:\*:\*:\*:\*:\*:\*