Security Bulletin

Updated 10/08/2022

Robustel has released a firmware security update for all RobustOS devices. This update addresses security issues in the RobustOS firmware that may lead to arbitrary command execution and arbitrary file deletion.
Please note that these issues require network access to the RobustOS device's web GUI and logging in to the RobustOS device with an account that has permission to edit functions.
This is generally not possible unless a Public IP SIM is being used so the scope of the real-world risk is very limited.

If you are using Public IP SIMs or you feel your architecture requires additional protection, please download and install this firmware update through the RCMS or Robustel official Website.

DETAILS

This section summarizes the potential impact that this security update addresses. Descriptions use CWE™, and base scores and vectors use CVSS3.0 standards.

CVE IDs	Summary	Base Score	Vector
CVE-2022-33329	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/set_sys_time/` API is affected by a command injection vulnerability.	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVE-2022-33328	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/remove/` API is affected by a command injection vulnerability.	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVE-2022-33327	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/remove_sniffer_raw_log/` API is affected by a command injection vulnerability.	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVE-2022-33326	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

	R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/config_rollback/` API is affected by a command injection vulnerability.		
CVE-2022-33325	Multiple command injection vulnerabilities exist in the web_server ajax endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network packets can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/ajax/clear_tools_log/` API is affected by command injection vulnerability.	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVE-2022-33314	Multiple command injection vulnerabilities exist in the web_server action endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/action/import_sdk_file/` API is affected by command injection vulnerability.	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVE-2022-33313	Multiple command injection vulnerabilities exist in the web_server action endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/action/import_https_cert_file/` API is affected by command injection vulnerability.	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVE-2022-33312	Multiple command injection vulnerabilities exist in the web_server action endpoints functionalities of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger these vulnerabilities.The `/action/import_cert_file/` API is affected by command injection vulnerability.	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVE-2022-32585	A command execution vulnerability exists in the clish art2 functionality of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	9.1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVE-2022-28127	A data removal vulnerability exists in the web_server /action/remove/ API functionality of Robustel R1510 3.3.0. A specially-crafted network request can lead to arbitrary file deletion. An attacker can send a sequence of requests to trigger this vulnerability.	8.7	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H

SECURITY UPDATES

The following table lists the products affected, versions affected, and the updated version that includes this security update.

Download the updates from the RCMS and Robustel official Website

CVE IDs Addressed	Vulnerablity Report Date	Product Name	Affected Versions	Updated Version
CVE-2022-33329	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-33328	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-33327	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-33326	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-33325	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-33314	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-33313	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-33312	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-32585	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0
CVE-2022-28127	June 30, 2022; 3:15:08 PM	All RobustOS Devices	V3.x.x	V5.0.0

MITIGATION

Upgrade to version 5.0.0

INITIAL PUBLICATION DATE

August 10th, 2022

REVISION HISTORY

Revision	Date	Description
1.0	August 10th, 2022	Initial release

SUPPORT

If you have any questions about this security bulletin, contact Robustel Support Team