CVE-2021-32030

ASUS Routers Improper Authentication Vulnerability

Exigent | CISA KEV since Jun 2, 2025 | Actively exploited

The administrator application on ASUS GT-AC2900 devices before 3.0.0.4.386.42643 and Lyra Mini before 3.0.0.4_384_46630 allows authentication bypass when processing remote input from an unauthenticated user, leading to unauthorized access to the administrator interface. This relates to handle_request in router/httpd/httpd.c and auth_check in web_hook.o. An attacker-supplied value of '\0' matches the device's default value of '\0' in some situations.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
88/100 Immediate priority	9.8 Critical · NVD	0.994 99.94th percentile · FIRST	Jun 23, 2025 KEV since 2025 · listed over a year

Signals behind the score

counted in the score | not counted — evidence for 6 of 8 signals

✓ CISA KEV	Listed in the catalog	− Vendor exploitation	Confirmed exploitation in the wild
− Ransomware	No known ransomware campaign association	− KEV recency	Added to CISA KEV within the last two years
✓ EPSS	0.994 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 9.8	− Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent — Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Note: All versions of Lyra Mini and earlier which are unsupported (End-of-Life, EOL) are also affected by this vulnerability, Consumers can mitigate this vulnerability by disabling the remote access features from WAN.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
lyra mini firmware	< 3.0.0.4.384.46630	3.0.0.4.384.46630	NVD
gt-ac2900 firmware	< 3.0.0.4.386.42643	3.0.0.4.386.42643	NVD
lyra mini	–	no fixed version listed	NVD
gt-ac2900	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-mmm5-f82c-58j8	asus.com	asus.com/us/supportonly/lyra%20mini/helpdesk_bios/
asus.com	asus.com/us/supportonly/rog%20rapture%20gt-ac2900/helpdesk_bios/	NVD	nvd.nist.gov/vuln/detail/CVE-2021-32030
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-18896
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-32030		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.