Early Warning Alert

ASUS ROUTER CRITICAL VULNERABILITIES

Summary	ASUS has published updated firmware with cumulative security updates that address vulnerabilities in several router models, advising customers to update their devices immediately or restrict WAN access until they are secure. According to the organisation, the newly released firmware fixes nine security flaws, including a high and critical one.
Technical Analysis	The most critical ASUS Router vulnerabilities are CVE-2022-26376 and CVE-2018-1160. The first vulnerability is a significant memory corruption flaw in the Asuswrt firmware for Asus routers, which could enable attackers to cause denial-of-service states or obtain code execution. The other important patch addresses a nearly five-year-old CVE-2018-1160 flaw caused by an out-of-bounds write Netatalk vulnerability that can likewise be used to gain arbitrary code execution on unpatched devices. If the updated firmware version is not installed, it is strongly advised to stop WAN-accessible services to avoid potential unwanted intrusions. Remote access from WAN, port forwarding, DDNS, VPN server, DMZ, and port trigger are all services that should be disabled. As an added layer of security, it is recommended that both equipment and security protocols be audited on a regular basis.
List of Affected Device	• GT6 • GT-AXE16000 • GT-AX11000 PRO • GT-AX6000 • GT-AX11000 • GS-AX5400

	• GS-AX3000 • XT9 • XT8 • XT8 V2 • RT-AX86U PRO • RT-AX86U • RT-AX86S • RT-AX82U • RT-AX58U • RT-AX3000 • TUF-AX6000 • TUF-AX5400
Conclusion	ASUS is known for being targeted by botnets before, hence this update firmware should be taken seriously. Some of the notable incident before was in March 2022, where Cyclops Blink malware attacks targeting multiple ASUS router models to gain persistence and use them for remote access into compromised network. Ergo, the purpose of this Early Warning Alert is to notify you of the most recent security vulnerability and its solution before a catastrophic incident happens.
Recommendation	FIRMUS recommends to • Update to the latest firmware via support website and each product's page for the affected devices • Create distinct passwords for wireless network and router administrator pages • Avoid using same password for multiple devices or services • Enable AiProtection for supported ASUS routers • Set up separate passwords for wireless network and Web GUI
Article Source	• https://www.bleepingcomputer.com/news/security/asus-urges-customers-to-patch-critical-router-vulnerabilities/ • https://www.asus.com/support/FAQ/1008000