CVE-2024-3596 (BlastRADIUS)

CVE-2024-3596 (https://www.blastradius.fail), also called BlastRADIUS is a vulnerability that enables a man-in-the-middle attack where RADIUS authentication response messages can be forged. This is not specific to any implementation of RADIUS but is a vulnerability in the RADIUS protocol itself. The following products are affected:

- Cambium Enterprise Wi-Fi APs, cnPilot E series Wi-Fi APs, Xirrus Wi-Fi APs and cnMatrix switches: the RADIUS client used on these products is affected. Cambium Enterprise Wi-Fi APs and cnPilot E series Wi-Fi APs are not affected when RADIUS is only used for 802.1X authentication (WPA/WPA2/WPA3 Enterprise).
- NSE 3000: The RADIUS server feature on NSE 3000 is affected when used for non-EAP authentication. It is not affected when used for EAP / 802.1X authentication
- cnMaestro on-premises: The RADIUS proxy feature and management user authentication using RADIUS is affected. cnMaestro on-premises is not affected if these features are not used. cnMaestro cloud is not affected.

We have no evidence of any other products being affected.

We recommend customers adhere to industry-standard best practices when using RADIUS including

- limiting RADIUS traffic to a management VLAN
- securing RADIUS traffic using IPSEC if it needs to traverse an untrusted network
- follow recommendations from your RADIUS server vendor to mitigate this vulnerability. Useful information for FreeRADIUS is available here https://www.freeradius.org/security/