Log4j Bulletin

Zetron is currently monitoring the following Apache Log4j Remote Code Execution Vulnerabilities:

- **CVE-2021-44228**
- **CVE-2021-45046**

We take the security of our products very seriously. Zetron has completed an assessment of our products based on the recommendations in the CVE.

Zetron's assessment has determined the following Zetron products are not impacted:

MAX Dispatch, MAX Call Taking, MAX Fire Station Alerting, ACOM, M6300 RoIP Gateway, Model 25 Programmable Encoder, Model 250 tone Remote Adapter, Model 284 Multi-line Tone Remote, Model 360 Kenwood-compatible Radio Remote, Model 4010/4010R Radio Dispatch Console, Pathway, Series 4000 Communications Control systems, IP-FSA, Series 2000 (includes M600/620/640), MT-4E

Zetron's assessment has determined the following products are impacted:

Cascade, UIC-5

The next Cascade release will include the recommended mitigation. A separate patch will be made available for the current UIC-5 release.

Zetron plans to monitor the evolving situation and publish updates as necessary. Customers with third-party products should refer to the individual manufacturers for updates regarding those products and implement mitigation measures in accordance with manufacturer guidelines.

We continue to recommend our customers follow cybersecurity best practices, including maintaining up-to-date software, antivirus, firewalls, device control, and usage policies to reduce the risk of cyber-attacks.

If you have questions, contact Zetron Technical Support:

Zetron Americas	Zetron EMEA	Zetron Australasia
+1 877 284 4616 (press 3) +1 425 820 6363 customercare@zetron.com	+44 1256 880663 emea@zetron.com	+61 7 3856 4888 ausales@zetron.com
6:00AM to 5:00PM PST 24-hour pager service available with service contract	8:00AM to 5:00PM GMT 24-hour pager service available with service contract	8:00AM to 5:00PM AEST (UTC +10 hours) 24-hour pager service available with service contract Standard Technical Support available M-F only