3 June 2024
RSSAC Caucus RSS Security Incident Reporting WP Call #23

18:15:28 From swoolf to Everyone:
It’s ok to have a category of another type of reportable incident, maybe a should-report incident rather than a must-report incident? But incident reporting is still separate to risk analysis, for instance such as what RSSAC undertook in the advisory about loss of a single server.
18:16:44 From Ken Renard to Everyone:
Section 4.3 "Operational Integrity"
18:17:21 From Ray Bellis to Everyone:
I was referring to the SOW itdelf
18:17:32 From Ken Renard to Everyone:
Reacted to "I was referring to..." with 👍
18:18:39 From Ray Bellis to Everyone:
And I’d read “operational integrity” being something that stops the RSS / an RSO from working at all, as opposed to maybe serving stale data.
18:21:28 From Ken Renard to Everyone:
I think the actions of the TLDs that delayed their roll-overs prevented the adverse effects
18:23:08 From Ray Bellis to Everyone:
FWIW, I do believe Cogent should provide more info and report as if this were a security incident, but I don’t think this WP’s current definition of “integrity” catches this class of issue.
18:24:36 From Duane Wessels, Verisign to Everyone:
I forgot something I wanted to add. IMO the Cogent incident does highlight that the publication latency metrics in 047 might not be ideal. We may want to re-open that in a future 047 work party.
18:24:45 From Ray Bellis to Everyone:
Reacted to "I forgot something I..." with 👍
18:25:18 From Wes Hardaker to Everyone:
I think both current events and the existince of this work party may end up pointing at other metric needs (aka: I agree Duane).
18:30:40 From Ray Bellis to Everyone:
Reacted to "I think both current..." with 👍
18:36:00 From Ray Bellis to Everyone:
I’m fine with what Paul is saying, but if we do this then I think our Terminology section needs updating too
18:37:27 From Ray Bellis to Everyone:
We should also remove “Security” from the document title ;-)
18:42:01 From swoolf to Everyone:
I might just be late to the party and missing the antecedents, but SLAs are probably going to require reporting of any SLA violation to the contract counterparty, presumably the RSS-GS. This is separate to deciding what incidents should be publicly reported.