GLOBAL RESILIENCE FEDERATION

May 2023 Newsletter

TLP CLEAR

IN THIS ISSUE: Summit Price Change, AI Webinar, K-12 Phishing

Price Change

The Summit on AI Security & Trust has just had a price change. Registration is now $495. ISAC and ISAO members may use discount code AI20 for 20% off at checkout. Join your peers in Washington, DC from June 7-9 to discuss one of the most promising and potentially problematic technology shifts of all time! Register and book a room soon though because the hotel room block closes May 17. Learn more

AI Webinar

Jonathan Dambrot, CEO of Cranium, and Andrew Moyad, CEO of Shared Assessments, joined GRF's Mark Orsi for a webinar on the threats and opportunities that come with increasing access to AI.

Both panelists flagged significant issues we'll have to grapple with as AI becomes more common. For example, says Moyad, Generative AI is turning attribution and the chain of custody on its head. How will we manage model risk in the future? What are the implications for traditional ways of thinking about CIA - Confidentiality, Integrity, and Availability?

Dambrot added that a year ago, attempts to have a discussion on AI security fell on deaf ears, even as enterprises were developing these ML/AI models outside security team visibility. Since that point there has been explosive user growth in the field. ChatGPT was, by total number of users, the fastest application to ever reach 100 million users. Now we need to reconcile development and security.

AI Webinar cont.

Watch the webinar "The Emergence of AI: New Opportunities and New Threats."

If this topic is of interest- or concern- join GRF in person for the upcoming Summit on AI Security & Trust, June 7-9 in Washington, DC. The summit is an opportunity to engage on an issue undergoing incredible growth that will have significant impact on operations and security.

The summit features 25+ speakers from nearly a dozen industries covering topics like consumer engagement with AI, balancing ROI vs. risk, the security of AI in physical systems, resilience in AI models, securing machine learning, and use of caution in AI-based decision making. Learn more

K12 SIX Members Briefed on Targeted Phishing

Content filters are useful in protecting students from dangerous or distracting parts of the internet, but they don't prevent them from falling victim to phishing attacks or accessing dangerous websites.

A recent K12 SIX TLP: AMBER briefing – delivered by Identity Automation – highlighted the tactics used by threat actors to bypass detection and keep malicious domains accessible to school members, as well as the ways students bypass school filters to access these dangerous websites.

Interested in becoming a member, sponsor, or partner? Contact info@grf.org.

DoS Attack, Supply Chain Exercise & Call for Speakers

DoS Vulnerability

A new reflective DoS amplification vulnerability, tracked as CVE-2023-29552, was reported in the Service Location Protocol (SLP) and allows threat actors to launch massive attacks with 2,200 times the amplification. BitSight and Curesec researchers say that over 2,000 organizations are using devices that expose roughly 54,000 exploitable SLP instances for use in DDoS amplification attacks. Vulnerable services include VMWare ESXi Hypervisors, Konica Minolta printers, IBM Integrated Management Modules, and Planex Routers deployed by organizations around the world.

According to BitSight, the most vulnerable instances are in the United States, Great Britain, Japan, Germany, Canada, France, Italy, Brazil, the Netherlands, and Spain, and are owned by several Fortune 1000 companies in technology, telecommunications, healthcare, insurance, finance, hospitality, and transportation.

This extremely high amplification factor allows for an under-resourced threat actor to have a significant impact on a targeted network and/or server. In an attack scenario, a threat actor would leverage multiple SLP instances to launch an attack, coordinating responses and overwhelming targets with traffic.

To protect your organization's assets from potential abuse, SLP should be disabled on systems exposed to the Internet or untrusted networks. If this is not possible, it is recommended to configure a firewall that filters traffic on UDP and TCP port 427.

Sample triggers in the supply chain exercise

Supply Chain Tabletop Exercise

Back by popular demand! The GRF Business Resilience Council is offering a second tabletop exercise exploring supply chain resilience and Business Continuity Management (BCM) implications in the event of a geopolitical conflict between Taiwan and China. The four hour exercise is scheduled for May 18. Members are encouraged to participate and contribute their expertise, including suggested injects. Contact cdenning@grf.org.

Sunny Austin, Texas

Call for Speakers

The 2023 Summit on Security & Third-Party Risk will be held October 11-12 in Austin, Texas. Submit your presentation topic today! Learn more

Community Contacts

OT-ISAC (John Lee)
LS-ISAO (Raquel Santiago)
EASE (Tim Chase)
ProSIX (Mark Orsi)
K12 SIX (Doug Levin)
BRC (Chris Denning)
Manufacturing ISAC (Tim Chase)
ONG-ISAC (Roderick Austin)
Newsletter contact (Pat McGlone)