RESCANA

Case Study: Rescana's Comprehensive Approach to Mitigating Third-Party Risks Following the Belsen Group's Fortinet Data Leak

Background

In January 2025, the Belsen Group, a newly identified hacking entity, publicly leaked configuration data and VPN credentials for over 15,000 Fortinet FortiGate firewalls. This data, reportedly obtained from a compromise dating back to 2022, was made available on the dark web, posing significant security risks to affected organizations and their third-party partners. citeturn0search0

Rescana's Immediate Actions

Upon learning of the leak, Rescana promptly initiated a comprehensive response to assist its clients and their third-party partners in mitigating potential threats:

1. **Identification of Affected Assets**: Rescana utilized its advanced asset discovery tools to identify clients' and their third-party partners' FortiGate devices potentially impacted by the leak. By cross-referencing the leaked IP addresses and configurations, Rescana ensured accurate identification of vulnerable assets.

2. **Vulnerability Assessment**: Leveraging its AI-driven vulnerability assessment platform, Rescana evaluated the security posture of the identified devices. This assessment focused on detecting the presence of the CVE-2022-40684 vulnerability, an authentication bypass flaw exploited by the Belsen Group. citeturn0search0

3. **Third-Party Risk Management (TPRM) Support**: Recognizing that clients' third-party partners could also be affected, Rescana extended its services to assess and mitigate risks within the broader supply chain. This proactive approach aimed to reduce third-party risk management (TPRM) concerns by ensuring that partners adhered to the same security standards.

4. **Patch Management Guidance**: Rescana provided clients and their third-party partners with detailed guidance on applying the necessary patches to remediate the CVE-2022-40684 vulnerability. This included step-by-step instructions and best practices to ensure the effective application of security updates.

5. **Credential Rotation Support**: Recognizing the risk posed by exposed VPN credentials, Rescana assisted clients and their partners in implementing comprehensive credential rotation strategies. This process involved updating administrative and VPN passwords to prevent unauthorized access.

6. **Continuous Monitoring and Threat Intelligence**: Rescana's platform offered continuous monitoring of clients' and their third-party partners' networks, alerting them to any suspicious activities or potential exploitation attempts. Additionally, Rescana provided real-time threat intelligence updates related to the Belsen Group's activities and emerging vulnerabilities.

Outcome

Through Rescana's proactive measures, clients and their third-party partners were able to swiftly identify and remediate vulnerabilities associated with the leaked FortiGate data. This comprehensive approach ensured that both primary and secondary networks remained secure, minimizing the risk of unauthorized access and potential data breaches.

Rescana is here for you!

Rescana's rapid and effective response to the Belsen Group's Fortinet data leak underscores the importance of proactive cybersecurity measures and robust third-party risk management. By leveraging advanced tools and providing expert guidance, Rescana enabled its clients and their partners to navigate the incident with confidence, reinforcing their overall security posture.