GE VERNOVA

PRODUCT & INFRASTRUCTURE PENETRATION TESTING

Software Development Lifecycle | Secure Development

PENETRATION TESTING OF GE VERNOVA PRODUCTS

GE Vernova's Threat Research Lab conducts security assessments on GE Vernova's products, solutions, and infrastructure.

GE Vernova also conducts external Third-Party testing on selected products and infrastructure adding depth to our security posture.

BUSINESS CHALLENGE

With some sources declaring over 2,000 cyber-attacks occur each day world-wide, GE Vernova has a rigorous penetration testing program in place.

GE Vernova has internal and external testers performing authorized simulated attacks as part of its larger Secure Development Lifecycle (SDL).

OVERVIEW

The GE Vernova Team

The Threat Research Lab (also known as GE Vernova's Red Team) employs security researchers having diverse experience protecting public and private entities and infrastructure from threat actors. Threat Research Lab members conduct research and assessments across GE Vernova's technology stack and have identified vulnerabilities published as CVEs related to third-party products.

GE Vernova Methodology

The assessments conducted by the Threat Research Lab are carried out using leading-edge testing and tools, including white box testing methodology. The Threat Research Lab receives complete access to the full suite of GE Vernova's products, including all sub-components and source code, and uses this access to enhance GE Vernova's ability to improve the security posture of its products, services, and overall assessment process.

The Threat Research Lab may simulate multiple threat actors, ranging from unprivileged attackers to malicious insiders with full access to a system. The assessment process starts by employing the standard penetration testing methodologies of enumeration and exploration of various entry points and moves on to an in-depth review of critical mechanisms, such as authentication and authorization, critical data flows, and similar high impact mechanisms. Due to the Threat Research Lab's familiarity with GE Vernova products, a body of proprietary knowledge has been amassed that allows the team to conduct security assessments with intimate knowledge of the system.

The Threat Research Lab's assessments are conducted on a quarterly and annual basis, with out-of-band testing conducted on sub-components undergoing major changes.

During the assessment, the Threat Research Lab's findings are promptly reported to GE Vernova's development teams. Each finding report contains a technical description of the finding, its impact on the system, severity score, steps required to reproduce the finding, and recommendations for mitigating it.

During the mitigation phase, the Threat Research Lab partners with GE Vernova's software developers to mitigate discovered findings. Following mitigation, major and critical findings are returned to the Threat Research Lab for validation of the applied remediations. These validations are conducted by the Threat Research Lab's researchers with input from the development team.

Assurance

To help ensure GE Vernova is able to protect its customers and their proprietary data stored on its systems, GE Vernova does not distribute details of testing nor the specific output of penetration testing. Visit GE Vernova's Cybersecurity Trust Center to learn more about the overall cybersecurity approaches GE Vernova employs and the cyber security certifications GE Vernova maintains. GE Vernova's cloud-hosted and software solutions are built on a common infrastructure governance model based on ISO 27001/2

Contact Us

ge.com/digital.sales-contact-me

Sources

https://us.norton.com/blog/emerging-threats/cybersecurity-statistics