A CONVERGE COMPANY

CASE STUDY

Manufacturer Uncovers Source Code Management and VPN Vulnerabilities

Challenge

An American automotive manufacturer had a new CISO who wanted to take a fresh, unbiased look at the efficacy of the organization's security controls. The company had worked with CBI, A Converge Company on its incident response readiness capabilities in the past. They were looking to evaluate defenses against the latest attacker tactics, techniques and procedures [TTPs], and identify any unknown attack surfaces.

Solution

Members of CBI's Advanced Testing Services [ATS] performed reconnaissance to determine the topology of the network and live hosts. Approximately 700 live hosts were found connected to external IP addresses among the 45,000 addresses that were in scope for the engagement. Enumeration of the hosts took place to identify operating systems, services, and protocols. Vulnerability scanning, port scanning, service identification, OS fingerprinting, and DNS enumeration techniques were used, and firewall and VPN penetration testing were carried out.

The client had strong controls in place, but open-source intelligence [OSINT] gathering revealed API keys for an Azure service that were exposed on GitHub. That issue, coupled with the discovery of a misconfigured extranet VPN used for non-employees and accessible with any password, enabled CBI to breach external network infrastructure.

After discovering and connecting to a Veeam backup service with credentials captured via a forced authentication attack and password cracking, our experts obtained data that enabled them to pivot to other machines as a local admin and access internal networks. Attackers using similar TTPs could gain control over most domain user accounts and access sensitive data.

Results

In order of priority, CBI provided an easy-to-read report containing an executive summary and risk-ranked descriptions of the vulnerabilities uncovered. The report detailed how vulnerabilities were exploited, and the exact steps required to remediate them.

The engagement complemented the organization's internal vulnerability management efforts and provided the objectivity needed to convey an accurate picture to key stakeholders. CBI manually retested after the remediation work was completed to verify vulnerabilities had been resolved.

Contact **CBI** to enhance your cybersecurity program.

800-747-8585 • help@cbisecure.com