issue 01

Discovery of an IoC

Case Study

ARCUS

arcusec.com

Client Overview

Arcus was engaged from a leading proctoring company to conduct a application penetration test. The scope of the penetration test covered the platform’s web application and API.

OBJECTIVE

The primary objective of the engagement was to identify and assess the security vulnerabilities within the organization's web application and deliver recommendations to protect against potential threats and to ensure the integrity, confidentiality, and availability of its data and systems.

ATTACK VECTOR

During the penetration testing process, Arcus' assessment team identified an insecure file upload feature within the client's web application. This vulnerability allowed malicious files to be uploaded to the server, bypassing the application's intended security controls. Utilizing this vulnerability, the team successfully uploaded a file that enables remote administration of the server.

The file provided the testers with significant control over the server, allowing them to execute arbitrary commands, access sensitive data, and further explore the network's security posture.

Through enumerating the host, the team discovered an indicator of compromise (IoC): evidence that a similar file had been uploaded by an unknown party. This finding suggested that the client's system had already been compromised, potentially exposing sensitive customer and company data to unauthorized access.

IMPACT

Data Breach Risk

The vulnerability exposed the client to the risk of a significant data breach, threatening customer privacy and financial information. Such breaches can result in substantial financial losses, legal penalties, and reputational damage.

Regulatory Compliance

The client was subject to strict regulatory requirements regarding data protection and cybersecurity. The identified vulnerabilities placed the client at risk of non-compliance, potentially leading to fines and sanctions.

Operational Disruption

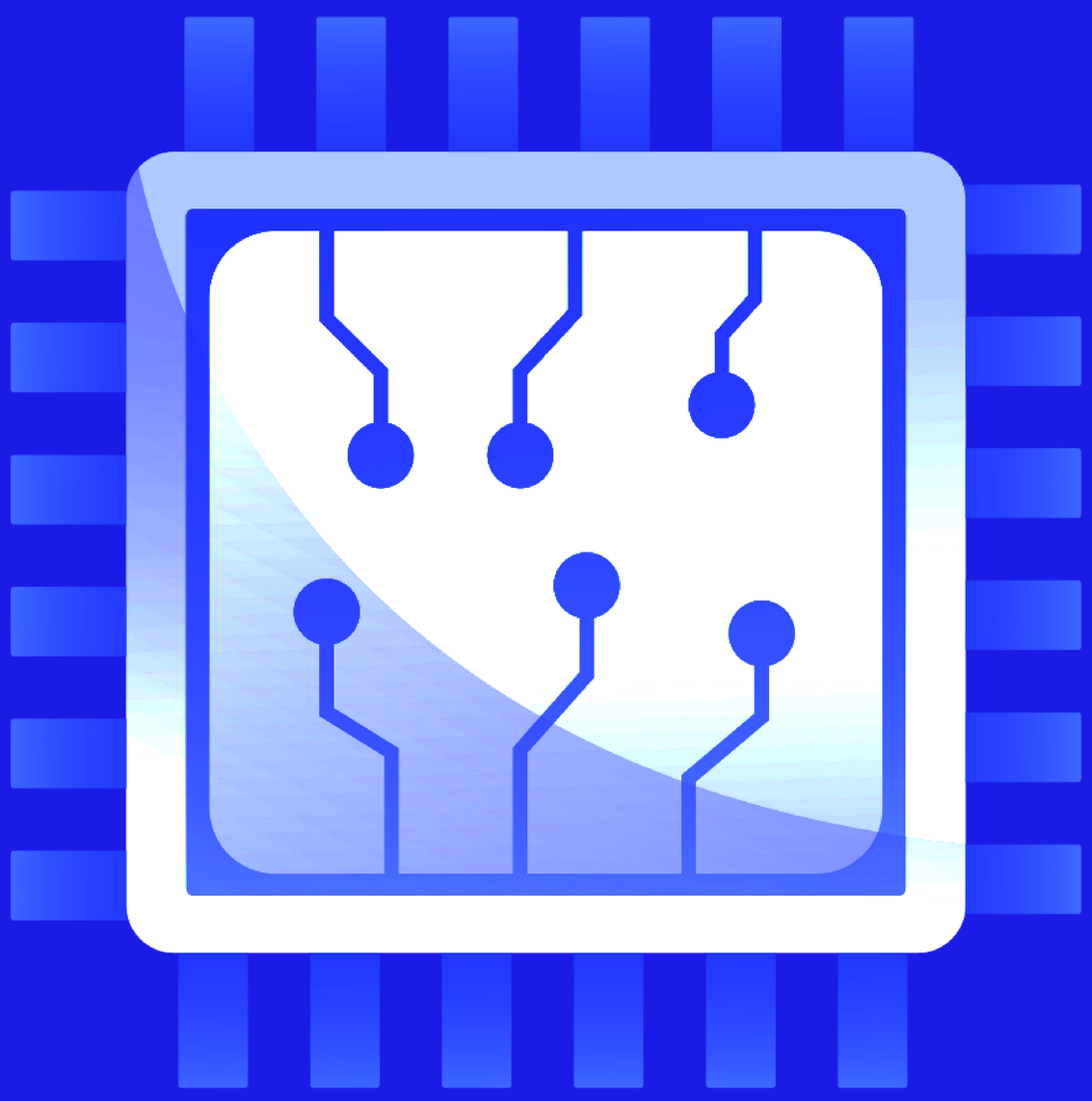
The exploitation of such vulnerabilities could lead to operational disruptions, affecting the client's ability to conduct business, service customers, and maintain financial transactions.

Reputational Damage

News of a cybersecurity vulnerability or actual breach can severely damage an organization's reputation, leading to lost trust among customers, partners, and stakeholders. The impact on customer confidence can have long-lasting effects on business performance.

Remediation Costs

Addressing any resultant breaches would incur significant costs, including technical remediation, legal expenses, and potential compensation for affected parties.



CONCLUSION

The average cost of a data breach in 2023 was USD **$4.45 million**. Hiring Arcus to perform penetration testing helps in proactively identifying and remediating vulnerabilities, significantly reducing the risk associated with such breaches.