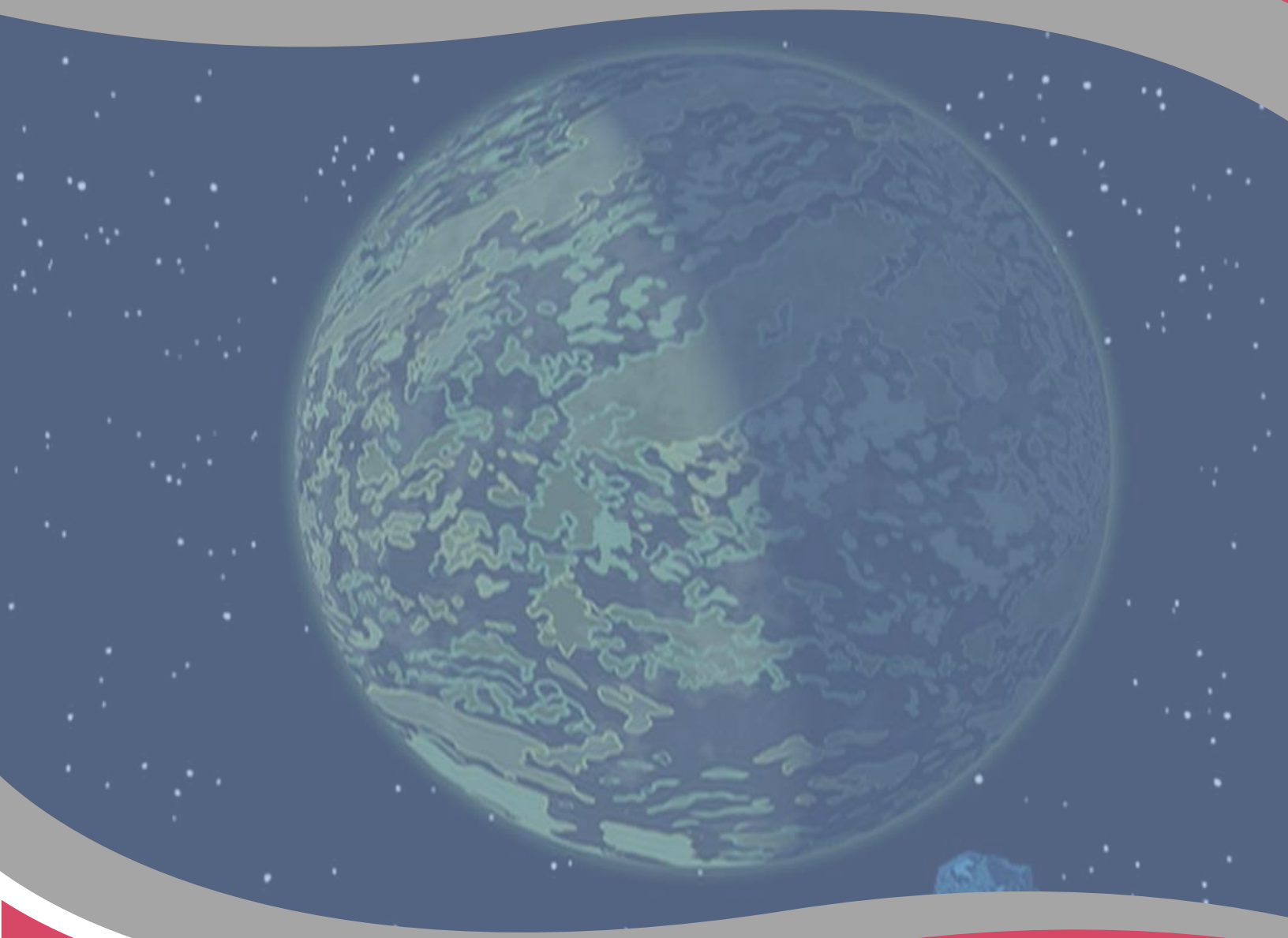
Penetration Test: Executive Report



Omicron Persei 8

Table of Contents

Introduction

As per the request from the planet of Omicron 8, a penetration test was commissioned to assess the security readiness of the web architecture and network infrastructure, ensuring they meet galaxy-wide standards. This initiative was prompted by internal concerns raised by the Information Technology team following recent cyberattacks on neighbouring planets. To prevent a similar disaster, Planet Express was contracted to conduct a penetration test on Omicron 8.

Objective

The aim of conducting a penetration test on a network is to pinpoint, exploit, and assess the security weaknesses within the network infrastructure. The primary purpose of this testing is to fortify the network's defences by detecting and resolving vulnerabilities before they are exploited by malicious entities, thus diminishing the overall risk exposure of the organization.

Findings

Upon completion of the penetration test, the Planet Express team found the following:

- 20 vulnerabilities on Omicron 8's network infrastructure
- 9 vulnerabilities on their primary website.

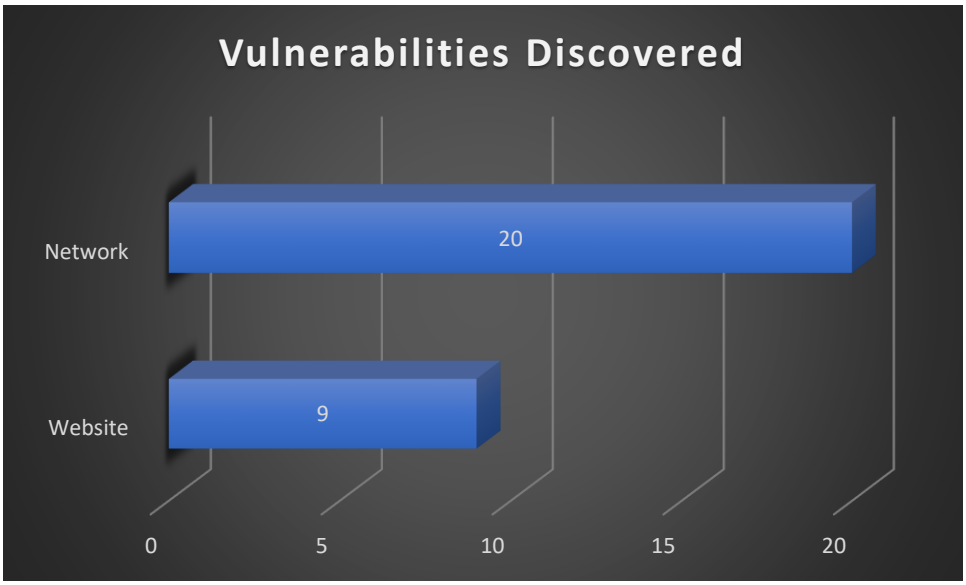


Figure 1 Total vulnerabilities discovered in Omicron Persei 8 IT infrastructure.

The following chart provides a visual guide of the risk levels of the vulnerability discussed in this report. Vulnerabilities labaled as CRITICAL should be remedied immediately, while those labeled as LOW are still be addressed but are not as high priority as the other risk levels.

Figure 2 Threat level of vulnerability.

The following pie charts show the threat levels of the vulnerabilities found on the network and primary website.

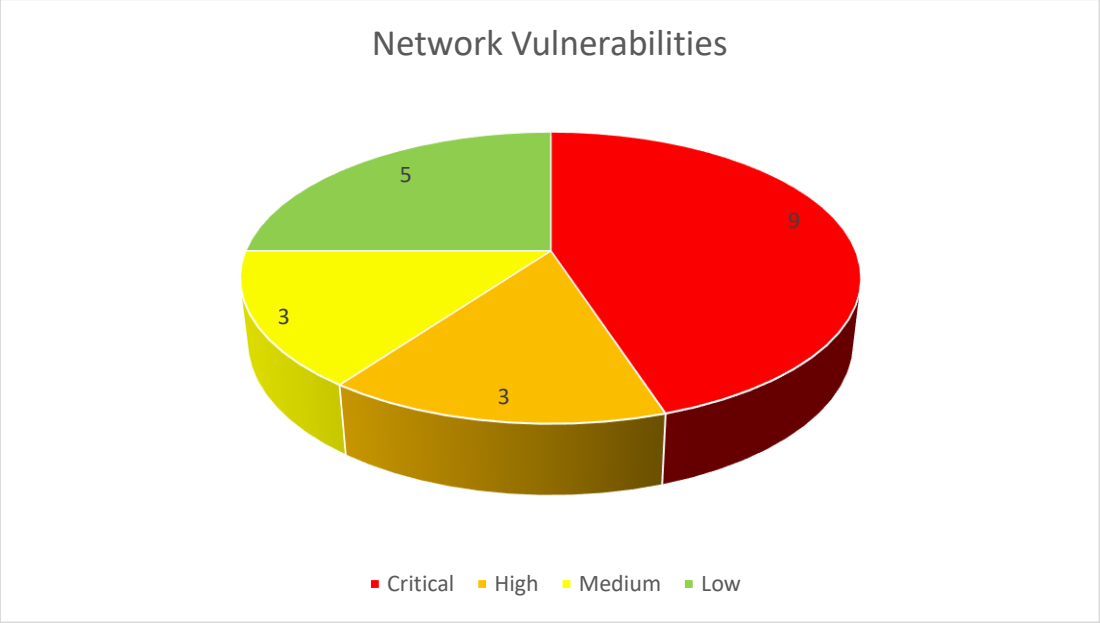


Figure 3 Threat levels of network vulnerabilities.

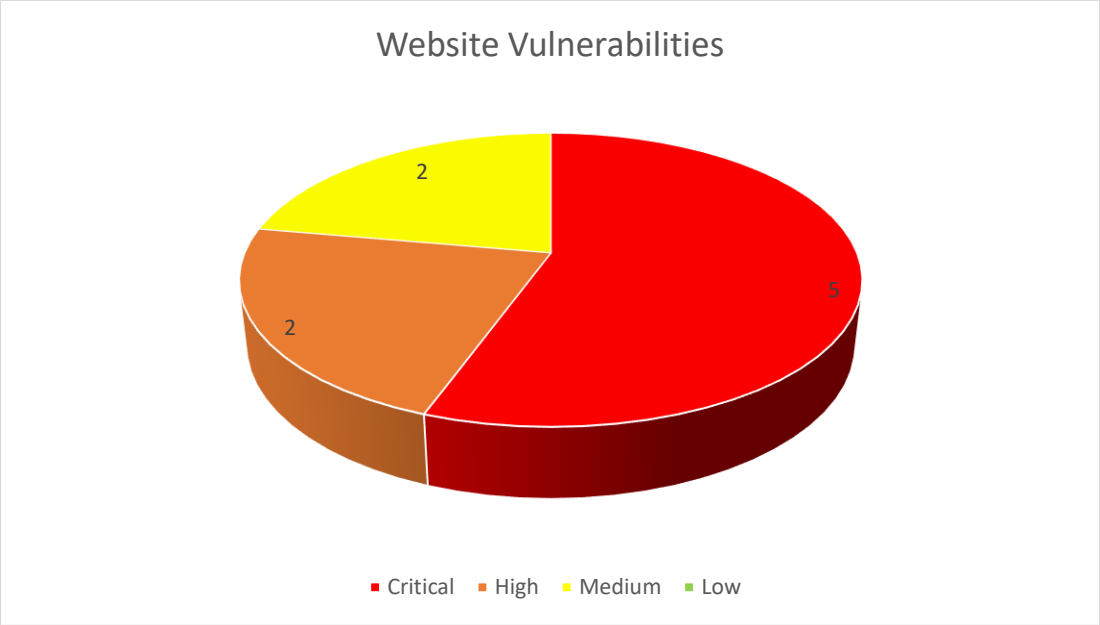


Figure 4 Threat levels of website vulnerabilities

The 20 vulnerabilities found on the network infrastructure, if left as it may lead to any number of the following:

- Brute force attacks
- Man-in-the-middle attacks
- Denial of service
- Credential theft and session hijacking.

The 9 vulnerabilities that were discovered on the primary website of Omicron 8 may lead to the following:

- Data breach
- Defacement
- Injection of malicious code
- Distributed denial of service attacks
- Malware distribution
- SEO Spam
- Loss of control of the website.

Recommendations

Planet Express recommends that these vulnerabilities be repaired as soon as possible, which will significantly improve Omicron 8's security posture. All vulnerabilities should be remedied in one month's time, with minimal disruption to daily services needed by Omicron 8.

Conclusion

Planet Express's penetration test revealed that Omicron Persei 8 does have security protocols and procedures in place for their network infrastructure and website architecture. However, our testing has shown several vulnerabilities that should be remedied as soon as possible given the current climate of planets being hacked. Remedying the vulnerabilities that are documented in this report should significantly improve the security posture of Omicron Persei 8 and keep it secure until the end of the year.