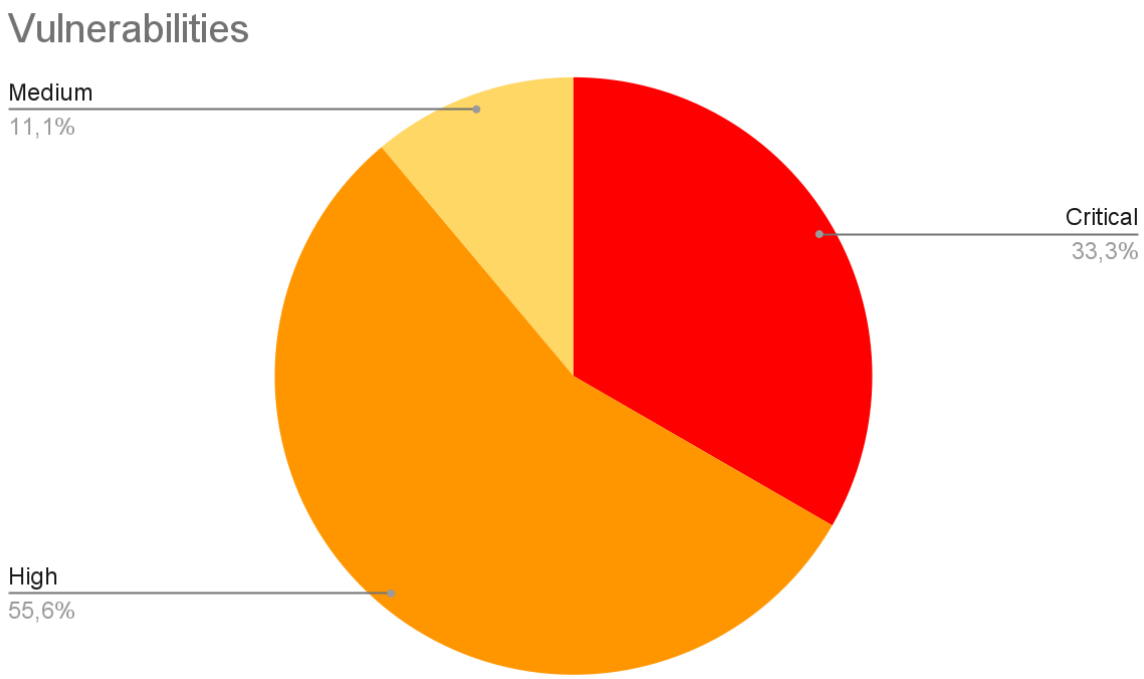
EXECUTIVE SUMMARY

Artemis Inc. engaged CyberHack Inc. to perform a penetration test at the risk of compromise from internal or external threats. The assessment took place in March 2025. The internal network was assessed using a laptop connected to the Artemis Inc. network. The external one was set from a computer in the CyberHack Inc. office. This information outlines the complete results of all recognized vulnerabilities and recommendations.

The current results reveal that Artemis Inc. has issues with the update and patching process and the network provisioning process, making the company susceptible to internal and external threats. CyberHack Inc. spotted three critical vulnerabilities on the internal network, five high and one medium on the external one.



To access to a full description of the pentesting process summarized here go to Capstone Rubric Phase 5: Detailed Technical Summary

Key Findings and Recommendations

- One of the Cisco appliances was added to the internal network without changing the default password. If this device stays in this condition, it can put the company in a vulnerable state, allowing intruders to manage traffic, deny service, and ultimately compromise the system.

  Recommendations

  This device's default password must be changed as soon as possible and should comply with the standard for secure passwords to make it difficult to crack.

- The Oracle WebLogic Server contains a vulnerability that allows intruders to compromise it through the HTTP protocol and potentially gain access to the corporate network.

  Recommendations

  This server should be patched as soon as possible. In the meantime, Port 7001 should be blocked or filtered to prevent harm.

- One Microsoft Exchange Server presents a vulnerability that allows unauthenticated users to send random HTTP requests to gain access to the server, allowing them to read sensitive information and possibly compromise the network.

  Recommendations

  This server should be patched as soon as possible to prevent attackers from exploiting it.

Conclusion

The assessment reveals that even though the company has a good level of cybersecurity, there is still room for improvement in updating and patching systems and network provisioning.