Inject #8: Risk Assessment

MAIL FROM: Team 1 “Club Penguin”
RCPT TO: Circle for the Protection of Antarctica
SUBJECT: Risk Assessment

Hello Circle For The Protection of Antarctica,

Risk Assessments are important in order to ensure that risk is being properly managed for that purpose. We have looked into 3 CVEs to best understand how to defend our topology.

CVE-2022-42247

This is a vulnerability that enables cross-site scripting in a php component. This means that an attacker could execute web scripts or HTML code on our topology via a crafted payload in a file name. Installing updates consistently for PFSense will allow us to mitigate this risk by allowing the developer to update the program correctly, removing the bug allowing this vulnerability.

CVE-2018-8649

This vulnerability creates a risk of denial of service for Windows mishandles an object in memory. This affects Windows 10 and Windows Server 2019. We can mitigate this risk by updating Windows in order to patch out the issue in question. Keeping the operating system updated ensures that as these vulnerabilities come up that they are handled before their risk can become a threat.

CVE-2022-1852

This vulnerability is a NULL point deference flaw in the Linux Kernel. This flaw occurs when executing illegal instruction in guest on an Intel CPU. This can result in a denial of service or execution of arbitrary code. This is a threat on our Linux boxes across the topology. Possible mitigations are firstly utilizing AMD CPUs instead of Intel CPUs, but more realistically keeping the Linux boxes upgraded as updates come out.

Regards,

Team 1 “Club Penguin”