Topic 4 Discussion 2

Research a critical vulnerability and exposure using the "CVE List Home," located in the topic Resources. Identify the CVE number and provide a link to the website. Assume your organization wishes the system to remain online and fully functional. Discuss in detail the specific vulnerability associated with your chosen list item, provide a plausible threat, and how you would mitigate it.

Hello Class,

Identified critical vulnerability, CVE-2023-26788

file location: https://nvd.nist.gov/vuln/detail/CVE-2023-26788.

This vulnerability was identified on 10 April 2023 by MITRE. (CVE-2023-26788, 2023) “Veritas Appliance is affected by host header injection attacks.” When the hypertext transfer protocol (HTTP) host header can be manipulated, it can cause the application to behave unexpectedly. For example, changes to the header would cause the request to be sent to a completely different Domain and IP address. The HTTP host header is a mandatory request header. It specifies the domain name that the client machine wants to access. If a request did not have a host header or have been manipulated, it would cause issues when routing incoming requests to the intended application. There are many ways to prevent host header attacks, including validating the host header against a whitelist, do not support host header override, whitelisting permitted domains, and being careful with internal-only virtual hosts. Validating the host header against a whitelist is checking against allowed fields and denying rejected or redirected connections. Host header override is when one deliberately overrides the host header for HTTPS/TLS.

References:

*CVE Website*. (2024). Cve.org. https://www.cve.org/CVERecord?id=CVE-2023-26788

*HTTP Host header attacks | Web Security Academy*. (n.d.). Portswigger.net. https://portswigger.net/web-security/host-header

Suryawanshi, T. (2023, April 13). *Understanding Host Header Injection Attacks and How to Prevent Them*. Medium. https://medium.com/@tushar\_rs\_/understanding-host-header-injection-attacks-and-how-to-prevent-them-60588cd34b8b