| **From**: Team #5 (Heads Empty)  **To**: CPA (The Circle for the Protection of Antarctica)  **Subject**: Inject #8  Hello again from Antarctica!  This is a Risk and Vulnerability report of three CVEs that are of high importance and ways to mitigate them (if applicable).  Common Vulnerabilities and Exposures (CVE) is a database of disseminated and cataloged security issues.   * Log4Shell also known as CVE-2021-44228 has a CVSS score of 9.3 and is a vulnerability in which an attacker that controls log messages can execute arbitrary code. This specific vulnerability affects Java, which is used by billions of applications and as a result makes this a serious threat. At the time of the creation of this report, the CVE has been mitigated and a patch is available. However, it requires a Java version of 2.17.1 (Java 8), 2.13.4 (Java 7) and 2.3.2 (Java 6) or above. It is highly recommended to update Java to the latest version to prevent Log4Shell exploits. Below is an article that details the CVE:   <https://www.cvedetails.com/cve/CVE-2021-44228/>   * A CVE posted in 2019 called CVE-2019-1020011 is a vulnerability that impacted confidentiality and integrity partially and has a CVSS score of 6.5. SmokeDetector is a project designed to detect spam, and would do deployments of updated copies of SmokeDetector without the server operator authority. Systems that have user accounts with limited permissions and system access are vulnerable to this vulnerability. A patch version has not been issued for this vulnerability according to their GitHub. Below is an article that describes the CVE:   <https://github.com/Charcoal-SE/SmokeDetector/security/advisories/GHSA-5w85-7mwr-v44q>   * A very new CVE known as CVE-2022-43571 has a CVSS score of 8.8 and is a remote code execution vulnerability. It can be exploited by authenticated attackers via PDF generation components within Splunk Enterprise. This vulnerability affects any system running Splunk Enterprise below the versions below 8.2.9, 8.1.12, and 9.0.2. This was a CVE recorded about one week ago from the time of this report. Despite this, Splunk has patched this vulnerability as well as nine other similar CVEs. These patches require the newest version of Splunk Enterprise, so it is highly recommended to update if needed. Below is an article detailing the CVE. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-43571>   We hope the CVEs listed above are recognized by your teams throughout the world and mitigated.    Sincerely,   * Heads Empty (ma13c, Ghost225, Ribs, Christippert, poseidon) |
| --- |