Unencrypted Network Traffic (version 1.0)

**Cloud Service Label: IaaS**

Description

Adversaries may be able to intercept network traffic. Some cloud services can utilize insecure comms that lead to plaintext information being transmitted. In some cases, the plaintext information being sent are credentials which may lead adversaries to gain access to specific cloud services, as well as, perform lateral movement.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Jenkins Azure AD Plugin | This [CVE](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2119) outlines a vulnerability in the Jenkins Azure AD Plugin 1.1.2 and earlier. The plain text credentials are transmitted as a global configuration form  resulting in possible exposure via intercepted network traffic, browser extensions, and cross-site scripting vulnerabilities. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| VPN | Utilizing a VPN can mitigate the risk due to application data being unencrypted. |
| Managed Service within Cloud Environment | Use a managed service over custom uploaded services or code within a cloud environment. Cloud service providers automatically update and patch their managed services whereas a custom service would have to be manually monitored and patched. |

Detection

This can be detected by monitoring network traffic to check for plaintext credentials when implementing new services or upgrading current services. Adversaries can also be detected if monitoring for rouge connections on the network.

References

1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2119. Accessed May 14, 2020.
2. <https://docs.aws.amazon.com/cli/latest/userguide/cli-security-enforcing-tls.html>. Accessed July 27, 2020.