Cory Wilson
NSS1501
Vulnerability Research

Vulnerability Name: CVE-2015-1310
Vulnerability Type: SQL Injection(CWE-89)
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Overview:

CVSS states that the vulnerability is an "SQL injection vulnerability in SAP Adaptive Server Enterprise (Sybase ASE) allows remote attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Note 2113333. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information."

Summary:

There was a vulnerability located within the SAP Sybase ASE Database Platform that allowed for a SQL Injection attack via the network vector. This allowed an attacker to write their own SQL queries at root level access and affect many processes within the database. They would have access to sensitive information, various administrator level actions, and could even disrupt the service entirely.

CVSS Score Breakdown:

- **Base Score:** 7.5
- **Exploitability Subscore:** 10
    - Access Vector: Network
    - Access Complexity: Low
    - Authentication: None
- **Impact Subscore:** 6.4
    - Confidentiality Impact: Partial
    - Integrity Impact: Partial
    - Availability Impact: Partial

Conclusion:

SQL Injection attacks can be devastating to a business and the SAP Sybase ASE Database Platform has a vulnerability allowing them to occur. It appears that SAP has rolled out a critical update patch that will help prevent this type of attack from occurring. The recommended course of action if you are utilizing this database platform is to install SAP Note.

Resources:

CVSS Entry

- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1310

CVSS Score Breakdown

- https://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2015-1310&vector=(AV:N/AC:L/Au:N/C:P/I:P/A:P)

ERPScan Article

- http://erpscan.com/press-center/blog/sap-critical-patch-update-january-2015/