# CVE Detail – CVE-2017-11508

SecurityCenter versions 5.5.0, 5.5.1 and 5.5.2 contain a SQL Injection vulnerability that could be exploited by an authenticated user with sufficient privileges to run diagnostic scans. An attacker could exploit this vulnerability by entering a crafted SQL query into the password field of a diagnostic scan within SecurityCenter. Successful exploitation of this vulnerability could allow an attacker to gain unauthorized access.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.62021

## CVSS Scoring

CVSS v3.0 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

## CAPEC(s)

* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-109: Object Relational Mapping Injection
* CAPEC-110: SQL Injection through SOAP Parameter Tampering
* CAPEC-470: Expanding Control over the Operating System from the Database
* CAPEC-66: SQL Injection
* CAPEC-7: Blind SQL Injection

## Affected Products

* cpe:2.3:a:tenable:securitycenter:5.5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:tenable:securitycenter:5.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:tenable:securitycenter:5.5.2:\*:\*:\*:\*:\*:\*:\*