Secunia Advisory ID	SA88121
Title	Flexera App Portal 2016 / 2017 / 2018 Multiple Vulnerabilities
Release date	2019-03-26
Last update	2019-04-15
Criticality	- Less critical
Impact	Manipulation of data, Cross Site Scripting
Where	From remote
Solution Status	Vendor Patched
Secunia CVSS Scores	CVSS3 Base: 6.1 , Overall: 5.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C
CVE references	CVE-2019-8958 | CVE-2019-8959 |

Affected operating system and software

Software

Flexera App Portal 2016

Flexera App Portal 2017

Flexera App Portal 2018

Advisory Details:

Description:

Multiple vulnerabilities have been reported in Flexera App Portal 2016, Flexera App Portal 2017, and Flexera App Portal 2018, which can be exploited by malicious users to conduct SQL injection attacks and by malicious people to conduct cross-site scripting attacks.

1) Certain input related to the "note context" parameter before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

2) Certain input related to the "MachineName" parameter is not properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerabilities are reported in versions 13.0 and prior.

Solution:

Update to version 14.0.

Provided and/or discovered by:

1) Abdullah H. AlJaber (aj.sa ; Twitter: @aljaber).
2) Mohammed Ababtain, Saudi Aramco.

Changelog:

2019-04-15: Updated credits.
2019-03-27: Updated credits.
2019-03-26: Updated credits.
2019-03-26: Initial release