



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

June 17, 2014

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2014-046

DATE(S) ISSUED:

06/17/2014

SUBJECT:

Multiple Vulnerabilities in Oracle Database Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

Multiple unspecified vulnerabilities have been discovered in Oracle Database that could allow remote code execution. Oracle Database is a database management system. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

Currently there are eight Proof of Concept (PoC) codes implementing three different privilege elevation techniques for gaining the administrator role in a target database environment. However, none of these PoCs are available publicly. Please note that patch is not available at this time.

SYSTEMS AFFECTED:

- Oracle Database 11g Release 2 (11.2.0.1.0) for Microsoft Windows x64
- Oracle Database 11g Release 2 (11.2.0.4.5) Patch Bundle 18590877 for Microsoft Windows x64
- Oracle Database 12c Release 1 (12.1.0.1.0) for Microsoft Windows x64
- Oracle Database 12c Release 1 (12.1.0.1.9) Bundle Patch 18724015 for Microsoft Windows x64

RISK:

Government:

- Large and medium government entities: High
- Small government entities: High

Businesses:

- Large and medium business entities: High
- Small business entities: High

Home users: N/A

TECHNICAL SUMMARY:

Twenty vulnerabilities have been reported for Oracle Database. Details of the vulnerabilities are not available at this time, however, it has been reported that a malicious user with the bare minimum privileges required to connect and login to Oracle Database can successfully execute arbitrary Java code on the Oracle Database.

Successful exploitation could result in an attacker gaining the same privileges as the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Update vulnerable Oracle Database products immediately after appropriate testing when a patch becomes available.
- Consider limiting access to Oracle Server until patch becomes available
- Consider implementing the CIS Benchmarks for Oracle Database Server

REFERENCES:

Full Disclosure:

<http://seclists.org/fulldisclosure/2014/Jun/79>

SecurityFocus:

<http://www.securityfocus.com/bid/68057>