

September 11, 2007

**CRITICAL**

# Security Analysis

---

## Oracle Jinitiator 1.1.8 Buffer Overflow Vulnerability Analysis

### OVERVIEW

US-CERT has released an advisory regarding multiple stack buffer overflows in the Oracle Jinitiator product ([Vulnerability Note VU#474433](#)). The information released by US-CERT is incomplete as to the true scope of vulnerable Jinitiator versions, does not properly identify all vulnerable Jinitiator installs, and has only limited remediation steps. In addition, the suggested remediation will break currently deployed applications that use Oracle Jinitiator 1.1.8.16.

All released Jinitiator 1.1.8 versions from 1.1.8.3 to 1.1.8.25 contain the buffer overflows in the Jinitiator ActiveX control – the US-CERT advisory only identifies versions through 1.1.8.16 as vulnerable. Each Jinitiator 1.1.8 version install uses a separate Microsoft Windows CLSID for the vulnerable ActiveX control to allow for multiple versions to co-exist, therefore, 15 CLSIDs must be used to disable the vulnerable ActiveX controls. In addition to disabling and uninstalling the vulnerable Jinitiator software, applications currently using vulnerable Jinitiator versions must be upgraded to use version 1.3.x which may also require upgrading the Oracle Forms software running on the server. It is important to note that each Jinitiator version (1.1.8.x) is a separate installation and there could be as many as 15 versions of Jinitiator 1.1.8 simultaneously installed on a client computer, even though only one or two versions are currently being used.

This analysis provides information on the true scope of affected Jinitiator versions, comprehensive and recommended remediation steps, and an overview of the risks associated with this vulnerability. The objective of this analysis is to assist IT security professionals, IT managers, and database administrators in assessing the impact on their Oracle Forms implementations and the risks associated with this vulnerability, especially since Jinitiator is deployed in many large organizations and as part of mission critical applications like the Oracle E-Business Suite, Oracle Clinical, and SunGard Banner.

### ORACLE JINITIATOR OVERVIEW

---

Oracle Jinitiator is an Oracle pre-packaged Java Virtual Machine (JVM) used by Oracle Forms applications. Oracle uses Jinitiator instead of the default JVM in order to provide a consistent JVM for a Forms application. For easy installation and to allow for direct execution from a browser session, Jinitiator installs an Internet Explorer ActiveX control and a Netscape plug-in (Mozilla, Netscape, and Firefox). Each Jinitiator version is certified for a specific Oracle Forms version (patchset), therefore, multiple Jinitiator subversions may be simultaneously installed on a client PC in order to support multiple Oracle Forms applications. Each installation is completely independent and newer versions never replace or uninstall any existing versions. As an example, versions 1.1.8.11, 1.1.8.25, and 1.3.1.9 may all be installed simultaneously. It is not uncommon in a large Oracle customer to have 5 or more Jinitiator versions installed on a client PC. There is no standard process to remove or uninstall obsolete or unused Jinitiator versions.

### **ACTIVEX CONTROL OVERVIEW**

To automate installation and execution of the Oracle supplied JVM, Jinitiator uses an ActiveX control. The ActiveX control is embedded as an OBJECT tag on a web page. The Object tag contains a Windows CLSID that uniquely identifies the Jinitiator ActiveX control. Upon encountering the OBJECT tag in a web page, Microsoft Internet Explorer (IE) will search for the CLSID of ActiveX control in the Windows registry. If the control is not found, IE will redirect the user to a web page to download the ActiveX control. In the case of Jinitiator, this is either a web page with download instructions or an install program such as "jinit11825.exe". If the control is found, then IE executes the control and passes parameters from the OBJECT tag on the web page to the control. As which point, the Jinitiator ActiveX control launches the Oracle JVM.

### **VULNERABILITY ANALYSIS**

---

A security researcher at US-CERT (Will Dormann) has discovered multiple buffer overflows in the processing of browser passed initialization parameters by the Jinitiator ActiveX control. These buffer overflows potentially allow an attacker to execute arbitrary code on the client PC if the attacker is able to lure the user into accessing the attacker's web page.

### **RISK ANALYSIS**

---

Wide exploitation of this vulnerability is unlikely due to the limited install-base of vulnerable Oracle Jinitiator versions. However, targeted attacks against known Oracle customers will probably be successful as vulnerable Jinitiator versions remain installed on client PCs indefinitely. Working with several large organizations in proof of concept testing of a targeted attack, we achieved high success rates in exploiting this vulnerability.

There are no statistics on the actual number of client PC installs of Jinitiator to determine the true extent of vulnerable client PCs. However, Google searches for download web pages of vulnerable Jinitiator 1.1.8 versions revealed hundreds of pages, especially many government agencies and higher education institutions.

### **REMEDIATION STEPS**

---

#### **STEP 1 – IDENTIFY AND INVENTORY ORACLE FORMS APPLICATIONS**

Before disabling or uninstalling vulnerable Oracle Jinitiator versions, you should ensure no current applications are using these versions. Oracle Forms applications may be large commercial applications like the Oracle E-Business Suite 11i, custom internally developed applications, or external partner or government applications. Oracle Forms has been popular with many government agencies to develop external applications and often these applications use older versions of Jinitiator. There is no simple method to inventory all such Oracle Forms applications within an organization or to identify external applications that may be accessed by a few individuals.

A few commercial applications using Oracle Jinitiator are –

- Oracle E-Business Suite 11.5.1 – 11.5.10.2
- Oracle Discoverer Plus

- Oracle Clinical
- Retek/Oracle Retail
- Sungard HE Banner 6/7
- i-Flex FLEXCUBE

Once an inventory is developed of Oracle Forms applications and the required Oracle Jinitiator versions, all 1.1.8 and prior versions should be upgraded to 1.3.1.29 or the latest supported version for the application and Oracle Forms version. All applications developed using Oracle9i Forms, Oracle Forms 10g, and Oracle Forms 10gR2 should be only using Jinitiator versions 1.3.1.9 and higher. Thus of primary concern are any applications currently using Oracle Forms6i, which supports both Jinitiator versions 1.1.8.x and 1.3.1.x. It is important to note that upgrading Jinitiator often requires Oracle Forms to be upgraded on the server.

Another option is to use the Sun JRE Plugin instead of Jinitiator, which is certified for some applications and versions of Oracle Forms.

If client PCs are inventoried to identify installed Jinitiator versions, the Jinitiator cache directory can be examined to determine if the Jinitiator version has been recently used. The directory "C:\PROGRAM FILES\ORACLE\JINITIATOR 1.1.8.x\JCACHE" contains cached JAR files from recently accessed applications. If the dates on any of the \*.I00 files are recent, then this version of Jinitiator has recently been used.

### **Oracle E-Business Suite Jinitiator Information**

Oracle Applications 11i should be upgraded to use Jinitiator version 1.3.1.29. See [Metalink Note ID 124606.1](#) for more information. An alternative is that 11i is certified to use the Sun JRE Plugin instead of Jinitiator, see [Metalink Note ID 290807.1](#) for more information. Oracle E-Business Suite R12 does not support Jinitiator 1.1.8, thus no action is required.

### ***STEP 2 – REMOVE OR DISABLE JINITIATOR 1.1.8 INSTALLS***

As previously discussed, each minor Jinitiator version is a separate install and must be removed and disabled individually. Each installation also installs a unique ActiveX control with a different CLSID. Theoretically, there could be as many as 15 installations of vulnerable Jinitiator versions on a single PC. We recommend that the vulnerable Jinitiator versions be uninstalled and also the ActiveX control be disabled in case a vulnerable version is re-installed.

### ***UNINSTALLING JINITIATOR***

The preferred remediation method is to uninstall unnecessary Jinitiator versions in order to remove the vulnerable ActiveX control and to eliminate potential future vulnerabilities. One area of concern is that Jinitiator also installs a Netscape plugin for use by Netscape, Mozilla, and Firefox.

Jinitiator 1.1.8.x can be removed through Microsoft Windows "Add or Remove Programs" in the Control Panel. The application name is "Oracle Jinitiator 1.1.8.x" where x may be 3, 7, 10, 11, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, or 25.

Jinitiator is installed using a standard InstallShield installation, thus can be remotely uninstalled using a standard method. The command line for the uninstall is as follows –

```
<windowsdir>\IsUninst.exe -y -a -m -f"C:\PROGRAM FILES\ORACLE\JINITIATOR 1.1.8.x\DeIsL1.isu"
```

where x may be 3, 7, 10, 11, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, or 25. Oracle Jinitiator is automatically installed from a website upon accessing the Oracle Forms application for the first time. The install process does allow the end-user to modify the installation path, therefore, the path "C:\PROGRAM FILES\ORACLE\JINITIATOR 1.1.8.x" is not guaranteed. The Jinitiator installation creates a unique Windows registry key with the path for each version. The registry key is as follows –

```
HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\Jinitiator\1.1.8.x\Home
```

### ***DISABLING THE ACTIVE X CONTROL***

The Oracle Jinitiator ActiveX control should be disabled in Windows to prevent it from being accessed from a webpage. This is the method described in the US-CERT advisory. Since each Jinitiator version ActiveX control uses a different Windows CLSID, all 15 potential versions should be disabled if they exist. For information on setting the kill bit, see [Microsoft Support Document 240797](#).

A sample registry script would be as follows for the Oracle Jinitiator 1.1.8.16 –

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{9b935470-ad4a-11d5-b63e-00c04faedb18}]
"Compatibility Flags"=dword:00000400
```

Based on the potential Oracle Jinitiator 1.1.8 versions installed, the following 15 CLSID should be used to disable all possible vulnerable versions of Oracle Jinitiator 1.1.8.

VERSION	CLSID	RELEASE DATE
1.1.8.3	A2001DD0-C7BD-11D4-A3E1-00C04FA32518	Dec 2000
1.1.8.7	FF348B6E-FD21-11D4-A3F0-00C04FA32518	Feb 2001
1.1.8.10	689FF870-2AC0-11D5-B634-00C04FAEDB18	
1.1.8.11	86ECB6A0-400A-11D5-B638-00C04FAEDB18	May 2001
1.1.8.13	ED54A7B0-6C1C-11D5-B63D-00C04FAEDB18	June 2001
1.1.8.14	0A454840-7232-11D5-B63D-00C04FAEDB18	July 2001
1.1.8.16	9B935470-AD4A-11D5-B63E-00C04FAEDB18	Sep 2001
1.1.8.18	1D2A8890-3083-11D6-B649-00C04FAEDB18	
1.1.8.19	5E2A3510-4371-11D6-B64C-00C04FAEDB18	Mar 2002
1.1.8.20	E2258010-B53C-11D6-B64D-00C04FAEDB18	Aug 2002
1.1.8.21	B5859259-C40B-4B2A-AF9D-3BF0F634B1D5	Dec 2002
1.1.8.22	332BD5A0-8000-11D7-B657-00C04FAEDB18	May 2003
1.1.8.23	B13D8B3E-04A8-406F-BD35-07530D4A62DC	Jan 2004
1.1.8.24	E79BC654-8FC6-4BB9-BFB8-8860779AE213	Jan 2004
1.1.8.25	7C2C94F0-7991-42B4-8D5F-4CB15B490657	Mar 2005

## ORACLE JINITIATOR 1.1.5 AND 1.1.7

---

Based on the original research performed by Will Dormann of the CERT/CC which has been validated by Integrity, all versions of Oracle Jinitiator 1.1.8 (1.1.8.3 through 1.1.8.25) are vulnerable to buffer overflows in multiple parameters. Our testing validates that Oracle Jinitiator 1.3.1.x versions are not vulnerable to these buffer overflows.

However, neither CERT/CC nor Integrity have tested for these buffer overflows in Oracle Jinitiator versions 1.1.5.x and 1.1.7.x, which were released between 1999 and 2001. We believe there is a high probability that these versions are also vulnerable to the identified buffer overflows. Due to the age of these versions, we have not included them previously in this document, but it may be prudent to also included these versions in any remediation process especially where older Oracle Forms applications (i.e., Oracle Forms 4.5) may be have been used (or are currently used) and client PCs are often in service more than 3 years.

VERSION	CLSID	RELEASE DATE
1.1.7.15.1 1.1.7.11 1.1.7.10 1.1.5.21.1	9F77A997-F0F3-11D1-9195-00C04FC990DC	May 1999
1.1.7.18	020F6116-407B-11D3-A3BB-00C04FA32518	Sept 1999
1.1.7.26	152AF7C0-B73A-11D3-A3D4-00C04FA32518	
1.1.7.27	093501CE-D290-11D3-A3D6-00C04FA32518	Dec 1999
1.1.7.28	AF9A5360-F528-11D3-A3DA-00C04FA32518	
1.1.7.30	21157916-4D49-11D4-A3E0-00C04FA32518	
1.1.7.31	AA44DA02-7F61-11D4-A3E1-00C04FA32518	
1.1.7.32	FF348B6E-FD21-11D4-A3F0-00C04FA32518	Feb 2001

## ORACLE JINITIATOR ACTIVE X CLSIDS

---

The following is a listing of the Oracle Jinitiator ActiveX CLSIDs versions 1.1.7.15.1 through 1.1.8.25 to allow for easy cut and paste (23 total) –

### **1.1.8.x**

A2001DD0-C7BD-11D4-A3E1-00C04FA32518  
FF348B6E-FD21-11D4-A3F0-00C04FA32518  
689FF870-2AC0-11D5-B634-00C04FAEDB18  
86ECB6A0-400A-11D5-B638-00C04FAEDB18  
ED54A7B0-6C1C-11D5-B63D-00C04FAEDB18  
0A454840-7232-11D5-B63D-00C04FAEDB18  
9B935470-AD4A-11D5-B63E-00C04FAEDB18  
1D2A8890-3083-11D6-B649-00C04FAEDB18  
5E2A3510-4371-11D6-B64C-00C04FAEDB18  
E2258010-B53C-11D6-B64D-00C04FAEDB18  
B5859259-C40B-4B2A-AF9D-3BF0F634B1D5  
332BD5A0-8000-11D7-B657-00C04FAEDB18  
B13D8B3E-04A8-406F-BD35-07530D4A62DC  
E79BC654-8FC6-4BB9-BFB8-8860779AE213  
7C2C94F0-7991-42B4-8D5F-4CB15B490657

### **1.1.5.x and 1.1.7.x**

9F77A997-F0F3-11D1-9195-00C04FC990DC  
020F6116-407B-11D3-A3BB-00C04FA32518  
152AF7C0-B73A-11D3-A3D4-00C04FA32518  
093501CE-D290-11D3-A3D6-00C04FA32518  
AF9A5360-F528-11D3-A3DA-00C04FA32518  
21157916-4D49-11D4-A3E0-00C04FA32518  
AA44DA02-7F61-11D4-A3E1-00C04FA32518  
FF348B6E-FD21-11D4-A3F0-00C04FA32518

## REFERENCES

### *JINITIATOR BUFFER OVERFLOW VULNERABILITY INFORMATION*

- US-CERT, [Vulnerability Note VU#474433](#), "Oracle JInitiator ActiveX control stack buffer overflows", 28 August 2007
- Common Vulnerabilities and Exposures (CVE), [CVE-2007-4467](#)
- National Vulnerability Database (NVD), [CVE-2007-4467](#)

### *ORACLE JINITIATOR INFORMATION*

- Jinitiator Download Page, <http://www.oracle.com/technology/software/products/developer/htdocs/jinit.htm>, 10 September 2007
- "JInitiator Versions and Corresponding Class Ids Required by MS Internet Explorer For Jinitiator 1.1.x", [Metalink Note ID 114391.1](#), 2 June 2006
- "Information on Earlier JInitiator Versions For Applications 11i", [Metalink Note ID 232200.1](#), 11 September 2007
- "Upgrading JInitiator with Oracle Applications 11i", [Metalink Note ID 124606.1](#), 6 September 2007
- "Information on Earlier JInitiator Versions For Applications 11i", [Metalink Note ID 232200.1](#), 11 September 2007
- "Upgrading Sun J2SE (Native Plug-in) with Oracle Applications 11i for Windows Clients", [Metalink Note ID 290807.1](#), 9 August 2007

## HISTORY

September 11, 2007 – Initial Version

## ABOUT INTEGRIGY

Integrigy Corporation is a leader in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. AppDefend is an intrusion prevention system for Oracle Applications and blocks common types of attacks against application servers. Integrigy Consulting offers security assessment services for leading ERP and CRM applications.

Integrigy's vulnerability scanner and auditing tool, AppSentry, has been updated to detect Oracle E-Business Suite 11i and Oracle Application Server implementations requiring vulnerable Jinitiator versions.

Integrigy Corporation  
P.O. Box 81545  
Chicago, Illinois 60602 USA  
888/542-4802  
[www.integrigy.com](http://www.integrigy.com)

Copyright © 2007 Integrigy Corporation.

Authors: Stephen Kost and Jack Kanter

If you have any questions, comments or suggestions regarding this document, please send them via e-mail to [alerts@integrigy.com](mailto:alerts@integrigy.com).

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise.

Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.

Integrigy's Vulnerability Disclosure Policy – Integrigy adheres to a strict disclosure policy for security vulnerabilities in order to protect our clients. We do not release detailed information regarding individual vulnerabilities and only provide information regarding vulnerabilities that is publicly available or readily discernable. We do not publish or distribute any type of exploit code. We provide verification or testing instructions for specific vulnerabilities only if the instructions do not disclose the exact vulnerability or if the information is publicly available.

Integrigy, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.