WebLogic Vulnerabilities
Oracle PeopleSoft Impact

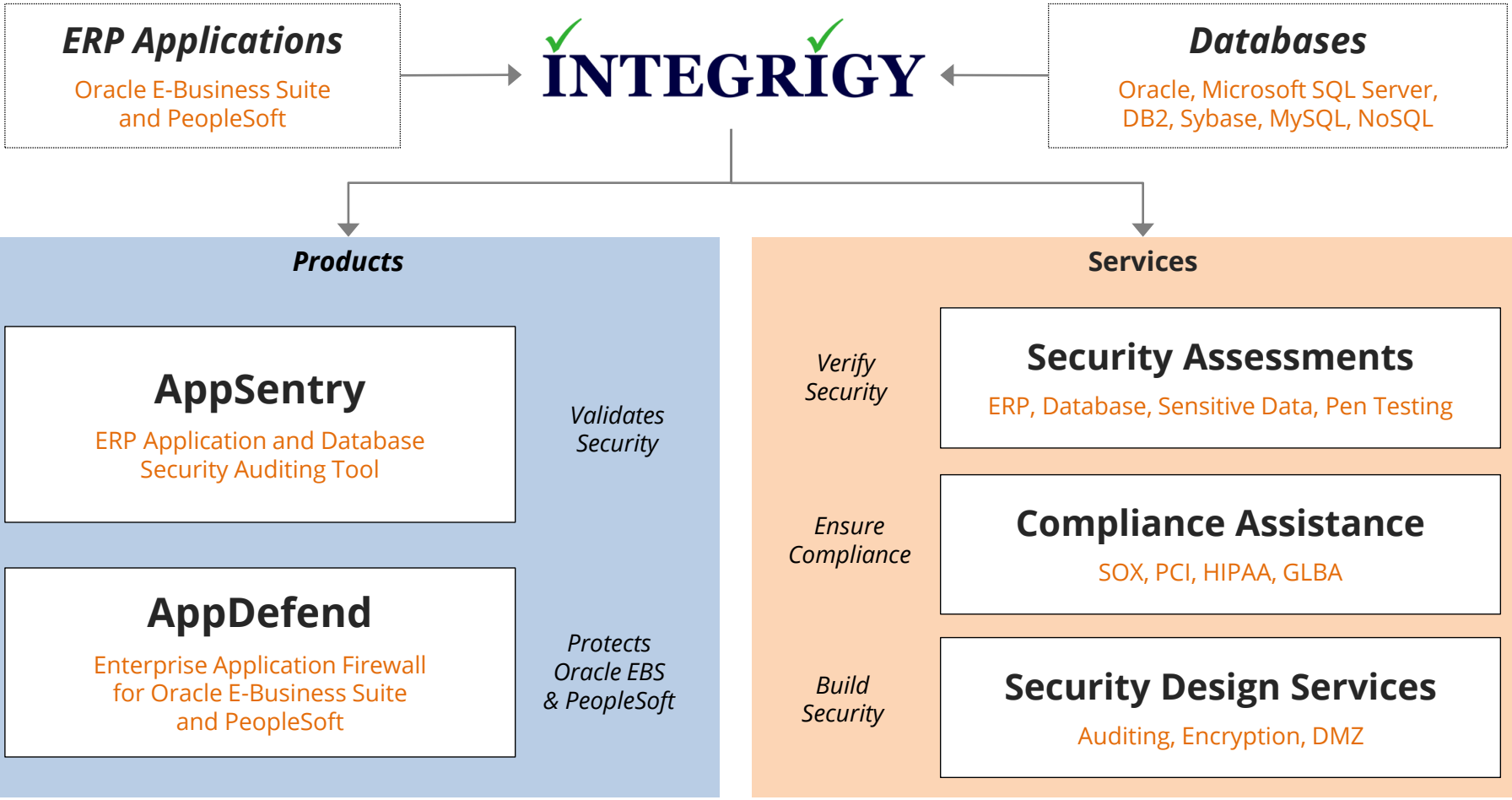
(CVE-2020-14882, CVE-2020-14883, CVE-2020-14750)

November 10, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

WebLogic Vulnerabilities 2020

	A CVE#	Product	B Component	Protocol	C Remote Exploit Without Auth.?	D CVSS Version 3.1 Risk: Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid	E Inte-grity	Avail	F Supported Versions Affected
Oracle Critical Patch Update (CPU) October 2020															
1	**CVE-2020-14882**	**Oracle WebLogic Server**	**Console**	HTTP	**Yes**	**9.8**	Network	Low	None	None	Un-changed	High	High	High	**10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0**
2	**CVE-2020-14883**	**Oracle WebLogic Server**	**Console**	HTTP	**No**	**7.2**	Network	Low	High	None	Un-changed	High	High	High	**10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0**
Oracle Security Alert (one-off) November 1, 2020															
3	**CVE-2020-14750**	**Oracle WebLogic Server**	**Console**	HTTP	**Yes**	**9.8**	Network	Low	None	None	Un-changed	High	High	High	**10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0**

A CVE (Common Vulnerability Enumeration) is a **standard numbering** of security vulnerabilities – search using Google or Twitter

B These vulnerabilities are limited to the WebLogic **Console** component

C If the vulnerability is remotely exploitable **without authentication**

D CVE Base Score is a scale of 1 to 10 with 10 meaning **entire server** can be compromised

E Attacker can **read and write to the server** and impact availability of the server

F Lists only **supported** versions of WebLogic which are vulnerable – all versions > 10.3.0 are vulnerable

WebLogic Vulnerabilities 2020

CVE-2020-14882	▪ Authorization bypass in WebLogic Console ▪ Classic **path traversal** vulnerability ▪ Full access to WebLogic Console with **no authentication**
CVE-2020-14883	▪ **Remote code execution** (RCE) vulnerability in WebLogic Console ▪ Allows execution of operating system commands by calling specific Java classes ▪ Requires authorization but can be used in combination with CVE-2020-14882
CVE-2020-14750	▪ Fix for CVE-2020-14882 which could be bypassed

CVE-2020-14882 Authorization Bypass URLs

- **WebLogic console URLs are –**
  - **/console/login/LoginForm.jsp** for login page
  - **/console/console.portal** for console once logged in
- **For Oracle E-Business Suite, the WebLogic console is running on a port such as 7001 and the URL would be something like –**
  - http://ps.example.com:8000/console/login/LoginForm.jsp for the login page
  - http://ps.example.com:8000/console/console.portal for the running logged in console
- **WebLogic authorization (login) can be bypassed by changing the URL and perform a path traversal using double encoding –**
  - /console/images/%252E%252E%252Fconsole.portal
  - /console/css/%252E%252E%252Fconsole.portal
  - /console/bea-helpsets/%252E%252E%252Fconsole.portal
- **WebLogic will decode the as follows –**
  - %252E%252E%252F → %2E%2E%2F → ../

Reference: https://owasp.org/www-community/Double_Encoding

CVE-2020-14883 OS Shell Execution

- The security bug is that a page in the WebLogic Console accepts a Java classname as input and executes this class
- Need to simply find a “helper” function that will do something you want, such as execute operating system commands
- There are is at least one very useful “helper” function in WebLogic Console but many others are possible –
  - `com.tangosol.coherence.mvel2.sh.ShellSession`

Example if running WebLogic on Windows –

```
handle=com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime.
getRuntime().exec('calc.exe');");
```

CVE-2020-14882 Issue and CVE-2020-14750 Fix

The first fix (CVE-2020-14882) is to check for –

/%252E%252E%252F

The issue is that lowercase works too –

/%252e%252e%252f

The second fix (CVE-2020-14750) is to check for –

/%252E%252E%252F

/%252e%252e%252f

WebLogic Vulnerability Demo

WebLogic Vulnerabilities 2020 Security Patches

Step 1 **CVE-2020-14882** **CVE-2020-14883**	WLS PATCH SET UPDATE OCT 2020 See MOS Note ID 1470197.1 *Patch Set Update (PSU) Release Listing for Oracle WebLogic Server (WLS)*
Step 2 **CVE-2020-14750**	WLS OVERLAY PATCH OCT 2020 PSU See MOS Note ID 2724951.1*Security Alert CVE-2020-14750 Patch Availability Document for Oracle WebLogic Server*

CVE-2020-14882 and CVE-2020-14750 Patch Tests

- **To verify the patches are properly applied, attempt to access the Console using the following URLs –**
  - /console/images/%252E%252E%252Fconsole.portal (CVE-2020-14882 test)
  - /console/images/%252e%252e%252fconsole.portal (CVE-2020-14750 test)
- **If 404 is returned, then patches are applied**
- **If the console is displayed (missing images), then patches not applied**
- **If the first URL returns 404 and the second URL returns the console page, then patch for CVE-2020-14750 is missing**

PeopleSoft WebLogic Managed Server Architecture

Single-Server	▪ WebLogic console deployed to **PIA** ▪ Same URL as PeopleSoft application
Multi-Server Domains	▪ WebLogic console deployed to **WebLogicAdmin** ▪ Default port is 9999 and allow all hosts ▪ WebLogic Node Manager runs only on WebLogicAdmin
Distributed Managed Servers	▪ An extension of Multi-Server Domains ▪ WebLogic Node Manager runs on each server

PeopleSoft WebLogic Console

Single-Server	▪ WebLogic console deployed to **PIA** ▪ **Block access to console (/console/*) externally** at load balancer or reverse proxy ▪ Review options to restrict access to console internally ▪ See MOS Note ID 2396558.1 *E-WL: How to Disable T3/T3S Protocol In Weblogic Used By PeopleSoft And Impacts Of Disabling It* Disable t3(s), ldap(s), and IIOP(s)
Multi-Server Domains/ Distributed Managed Servers	▪ As WebLogicAdmin is a separate domain, use domain connection filters to block access to the console WebLogic console → Domain → Security → Filter ▪ Restrict access to http(s), t3(s), ldap(s) and IIOP(s) protocols ▪ See MOS Note ID 2396558.1 *E-WL: How to Disable T3/T3S Protocol In Weblogic Used By PeopleSoft And Impacts Of Disabling It*

WebLogic Connection Filters

- **Defined under WebLogic console → Domain → Security → Filter**
- **Set Connection Filter to weblogic.security.net.ConnectionFilterImpl**
- **Set Connection filter rules like the following**
  - Rules are processed in order
  - Use IP addresses whenever possible to avoid DNS lookups

Allow server

127.0.0.1 * * allow https t3s

<server ip address> * * allow https t3s

Block all other (last rule)

0.0.0.0/0 * * deny http https t3 t3s ldap ldaps iiop iiops

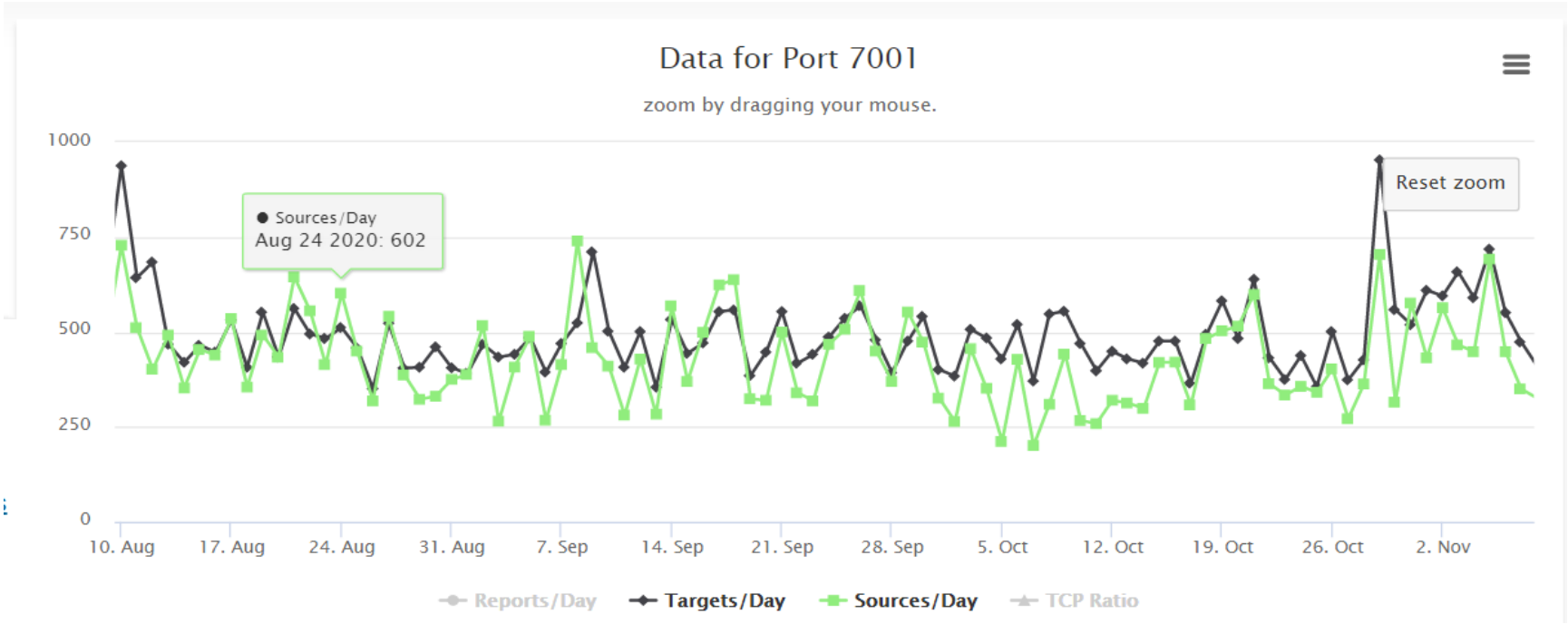
- **If using WLST for scripting, then t3/t3s must be enabled**

Finding WebLogic Servers

- **Attackers actively search for vulnerable servers on the Internet**
  - Use security search engines
  - Crawl the Internet (IP address by IP address)
- **Security search engines allow for searches by server type (WebLogic) and port number (7001)**
  - Shodan – https://www.shodan.io/
  - Censys – https://censys.io/
  - Spyse – https://spyse.com
- **Newer versions of PeopleSoft and Oracle E-Business Suite do not show WebLogic as the server type and should not appear in results**
  - Server string is set to empty since Oracle EBS 12.1.1

WebLogic Attacks and Port 7001

- Internet Storm Center (ISC) tracks through sensors on the Internet scanning for ports and attacks against servers
- There is active scanning for port 7001 and active attacks against using these WebLogic vulnerabilities



Source: https://isc.sans.edu/port.html?port=7001
Reference: https://isc.sans.edu/forums/diary/Cryptojacking+Targeting+WebLogic+TCP7001/26768/
Reference: https://isc.sans.edu/forums/diary/Attackers+Exploiting+WebLogic+Servers+via+CVE202014882+to+install+Cobalt+Strike/26752/

PeoplSoft Infrastructure Products

The following Oracle Fusion Middleware products use Oracle WebLogic –

- **Oracle Business Intelligence (OBIEE)**
- **Oracle Coherence**
- **Oracle SOA Suite**
- **Oracle Identity Management**
  - Oracle Internet Directory
  - Oracle Access Manager
  - Oracle Unified Directory

WebLogic Vulnerabilities in the Future

- **21 security researchers credited with finding these bugs**
  - They will not stop at this bug
  - Actively working to find the next "hot" WebLogic vulnerability
  - Able to sell such vulnerabilities to services or monetize through bug bounties ($$$)

- **Integrigy anticipates that a number of high-risk WebLogic vulnerabilities will be found and patched in future Oracle Critical Patch Updates**
  - Security bugs most likely will be in core WebLogic components such as Console
  - Core components are in all WebLogic implementations including Oracle EBS, PeopleSoft, OBIEE, SOA, Identity Management, etc.

- **WebLogic must be proactively hardened and protected**
  - Block access to everything except what you absolutely need
  - Use native WebLogic security features
  - Use web application firewalls (WAF)
  - Use load balancer/reverse proxy

Integrigy AppDefend

AppDefend is an **enterprise application firewall** designed and optimized for the PeopleSoft.

- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and published PeopleSoft vulnerabilities
- **Protects Web Services**
  Detects and reacts to attacks against native web services (SOA, SOAP, REST)
- **Application Logging**
  Enhanced application logging for compliance requirements like SOX, GDPR, PCI-DSS 10.2
- **Two-factor Authentication (2FA)**
  Enables two-factor authentication for login, user, responsibility, or function

Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**