Oracle Integrated Lights Out Manager

Security Configuration Supplement for the United States Department of Defense

ORACLE WHITE PAPER | OCTOBER 2014

Table of Contents

Overview

United States Department of Defense (DoD) Instruction 8500.01 (effective March 2014) instructs DoD Component Heads to "ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs with any exceptions documented and approved by the responsible authorizing official (AO)." Within the DoD, Security Technical Implementation Guides (STIGs) help to define the security configuration baselines for IA and IA-enabled devices. Specifically, STIGs contain prescriptive steps that can be used to both assess and improve the security configuration of systems and devices deployed on DoD networks. For more information on DoD STIGs, see: http://iase.disa.mil/stigs/Pages/index.aspx.

As of this white paper's publication, STIGs can only be developed when they align to one of the published DoD Security Requirements Guides (SRGs) per the STIG development vendor process, documented at: http://iase.disa.mil/stigs/Pages/vendor-process.aspx. Unfortunately, while the published SRGs map to common technology areas, there is no suitable SRG for IT appliances. As a result, there is no published STIG for the Oracle Integrated Lights Out Manager (ILOM) product as it is a dedicated, fixed-function appliance.

To mitigate this shortcoming, this technical white paper will provide prescriptive security configuration hardening guidance that will allow DoD customers to improve upon the default security configuration of Oracle ILOM in a manner suitable to what would otherwise have been published as a DoD STIG.

Product Description

The Oracle ILOM provides advanced service processor hardware and software that can be used to manage and monitor Oracle Sun servers. Oracle ILOM's dedicated hardware and software is pre-installed on Oracle's Sun server platforms including SPARC and x86-based servers as well as on Oracle appliances such as Oracle Exadata Storage Servers, Oracle ZFS Storage Appliance, as well as a variety of Oracle InfiniBand and Ethernet switches. The Oracle ILOM enables customers to actively manage and monitor the underlying server independently of the operating system state, providing a reliable lights out management capability. With Oracle ILOM, customers can:

» Learn about hardware errors and faults as they occur

» Remotely control the power state of the server platform

» Access the console of the server platform using graphical and non-graphical means

» Determine the hardware inventory and configuration of the system

» Receive generated alerts about system events

» Monitor environmental and power conditions

Product Security Guide

This white paper is intended to provide common information and procedures necessary to improve the "out of the box" security configuration of this product. The Oracle Integrated Lights Out Manager security guide, available as a standard part of the Oracle product documentation, has additional information on the product's security features, capabilities and configuration options. It is strongly recommended that customers review the product security guide before implementing the recommendations contained within this technical white paper.

» Oracle Integrated Lights Out Manager (ILOM) 3.2 Security Guide
http://docs.oracle.com/cd/E37444_01/pdf/E37451.pdf

» Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide
http://docs.oracle.com/cd/E24707_01/pdf/E24526.pdf

Always review the correct version of the product security guide as the security features, capabilities and configuration options will often vary based upon product version.

Version and Update Information

To leverage the most recent features, capabilities and security enhancements, customers are encouraged to update their Oracle ILOM software to the latest, supported version for their respective platform. To determine the version of the Oracle ILOM software that is being used on the platform, execute the following command after first logging into the Oracle ILOM.

```
-> version
SP firmware 3.2.1.5.b
SP firmware build number: 83085
SP firmware date: Tue Aug 13 09:07:24 PDT 2013
SP filesystem version: 0.2.7
```

In the above example, the Oracle ILOM software is version `3.2.1.5.b`. For detailed instructions describing how to update the Oracle ILOM software, refer to the "Performing Firmware Updates" section of the Oracle Integrated Lights Out Manager Configuration and Maintenance Guide. Note that for Oracle Engineered Systems such as the Oracle Exadata Database Machine or Oracle SuperCluster, additional restrictions may limit what versions of the Oracle ILOM software that can be used as well as how those versions are updated. In these situations, refer to the Oracle Engineered System product documentation to understand the process for updating system components.

Security Configuration Information

Default Accounts and Passwords

This section describes the default accounts and passwords associated with this device:

ORACLE ILOM DEFAULT ACCOUNTS AND PASSWORDS

Account Name	Account Type	Default Password	Account Description
`root`	Administrator	`changeme`	This is the sole default account that is delivered and enabled with this product. This account is used to perform initial configuration as well as to permit the creation of additional, non-shared administrative accounts. Note that the Oracle ILOM requires that the default password be changed immediately after the first successful login.

To list the accounts currently configured on the system, log into the Oracle ILOM and run the following command:

```
-> show /SP/users
```

To set the password for the root account, use the following commands:

```
-> set /SP/users/root password=<value>
```

Note that the Oracle ILOM does not have the ability to define or enforce password complexity, aging, history or other rules. Customers are encouraged to ensure that passwords assigned comply with DoD password complexity requirements and processes are implemented to ensure passwords are updated in accordance with DoD policy.

For more information on Oracle ILOM account management including how to create new accounts, assign permissions to existing accounts, or remove accounts, see the Oracle Integrated Lights Out Manager Configuration and Maintenance Guide at: http://docs.oracle.com/cd/E24707_01/pdf/E24522.pdf.

Default Exposed Network Services

This section describes the default network services that are exposed by this device:

ORACLE ILOM DEFAULT EXPOSED NETWORK SERVICES

Service Name	Protocol	Port	Service Description
SSH	TCP	22	This port is used by the integrated Secure Shell service to enable administrative access to the Oracle ILOM using a command-line interface.
HTTP (BUI)	TCP	80	This port is used by the integrated HTTP service to enable administrative access to the Oracle ILOM using a browser interface. While TCP/80 is typically used for clear-text access, by default the Oracle ILOM will automatically redirect incoming requests to the secure version of this service running on TCP/443.
NTP	UDP	123	This port is used by the integrated Network Time Protocol (NTP) (client only) service used to synchronize the local system clock to one or more external time sources.
SNMP	UDP	161	This port is used by the integrated SNMP service to provide a management interface to monitor the health of the Oracle ILOM and to monitor received trap notifications.
HTTPS (BUI)	TCP	443	This port is used by the integrated HTTPS service to enable administrative access to the Oracle ILOM over an encrypted (SSL/TLS) channel using a browser interface.
IPMI	TCP	623	This port is used by the integrated Intelligence Platform Management Interface (IPMI) service to provide a computer interface for various monitoring and management functions. This service is should not be disabled as it is used by Oracle Enterprise Manager Ops Center to collect hardware inventory data, field replaceable unit descriptions, hardware sensor information, and hardware component status information.
Remote KVMS	TCP	5120 5121 5123 5555 5556 7578 7579	Collectively, the Remote KVMS ports provide a set of protocols that provide remote keyboard, video, mouse and storage capabilities that can be used with the Oracle Integrated Lights Out Manager.
ServiceTag	TCP	6481	This port is used by the Oracle ServiceTag service. This is an Oracle discovery protocol used to identify servers and facilitate service requests. This service is used by products such as Oracle Enterprise Manager Ops Center to discover Oracle ILOM software and to integrate with other Oracle automatic service solutions.

`WS-Man over HTTPS`	TCP	`8888`	This port is used by the integrated WS-Man service to provide a standards-based, web-services interface that is used to manage the Oracle ILOM over the HTTPS protocol. Disabling this service will prevent the Oracle ILOM from being managed using this protocol.
`WS-Man over HTTP`	TCP	`8889`	This port is used by the integrated WS-Man service to provide a standards-based, web-services interface that is used to manage the Oracle ILOM over the HTTP protocol. Disabling this service will prevent the Oracle ILOM from being managed using this protocol.
`Single Sign On`	TCP	`11626`	This port is used by the integrated Sign Sign On feature that reduces the number of times a user has to enter a username and password. Disabling this service will prevent launching KVMS without having to re-enter a password.

For additional information on these services, refer to the Oracle ILOM security guide referenced above.

Security Configuration Hardening

Disable Unnecessary Services

It is recommended that customers disable any services that are not required to support the operational and management requirements of the platform. By default, the Oracle Integrated Lights Out Manager employs a network "secure by default" configuration whereby non-essential services are already disabled by default. That said, based upon customer security policies and requirements, it may be necessary to disable additional services.

To determine the list of services supported by the Oracle ILOM, use the command:

```
-> show /SP/services
```

To determine if a given service is enabled, use the command, substituting the parameter `<servicename>` with the name of a service returned using the previous command:

```
-> show /SP/services/<servicename> servicestate
```

While the majority of services recognize and use the `servicestate` parameter to record whether the service is enabled or disabled, there are a few services such as `servicetag`, `ssh`, `sso`, and `wsman` that use a parameter called `state`. Regardless of the actual parameter used, a service is enabled if the service state parameter returns a value of `enabled` as in the following examples:

```
-> show /SP/services/https servicestate

  /SP/services/https
    Properties:
        servicestate = enabled
```

```
-> show /SP/services/ssh state

  /SP/services/ssh
    Properties:
        state = enabled
```

To disable a service that is no longer required, set the service state to `disabled` using a command such as:

```
-> set /SP/services/http servicestate=disabled
```

As noted above, the Oracle ILOM is delivered in a network secure by default state where non-essential services are disabled by default. That said, depending upon the tools and methods used, the following additional services may be disabled if they are not required or used:

- Browser Administrative Interface (HTTP, HTTPS)

```
-> set /SP/services/http servicestate=disabled
-> set /SP/services/http secureredirect=disabled
-> set /SP/services/https servicestate=disabled
```

- Keyboard, Video, Mouse Service (KVMS)

```
-> set /SP/services/kvms servicestate=disabled
```

- Web Services Management (WS-Man over HTTP/HTTPS)

```
-> set /SP/services/wsman state=disabled
```

- Single-Sign On Services (SSO)

```
-> set /SP/services/sso state=disabled
```

Configure HTTP Redirection to HTTPS

By default, the Oracle ILOM is configured to redirect incoming HTTP requests to the HTTPS service to ensure that all of the communications are encrypted between the Oracle ILOM and the administrator. To verify that secure redirection is enabled, use the command:

```
-> show /SP/services/http secureredirect

  /SP/services/https
    Properties:
        secureredirect = enabled
```

If the default has been changed, secure redirection can be re-enabled using the command:

```
-> set /SP/services/http secureredirect=enabled
```

Disable Unapproved SSL/TLS Protocols

By default, the SSLv3 and TLSv1.0 protocols are enabled for the HTTPS service that is used to manage the Oracle ILOM. Customers may disable SSL protocol versions that do not comply with their security policy. To determine which SSL and TLS versions are enabled for the HTTP service, use the command:

```
-> show /SP/services/https sslv2 sslv3 tlsv1

  /SP/services/https
    Properties:
        sslv2 = disabled
        sslv3 = enabled
        tlsv1 = enabled
```

It is recommended that both SSLv2 and SSLv3 be disabled if not otherwise required. To disable SSLv2 and SSLv3, use the commands:

```
-> set /SP/services/https sslv2=disabled
-> set /SP/services/https sslv3=disabled
```

Disable SSL Weak and Medium Strength Ciphers

By default, Oracle ILOM disables the use of weak and medium strength ciphers for the HTTPS service that is used to manage the Oracle ILOM. To determine if weak and medium strength ciphers are disabled, use the command:

```
-> show /SP/services/https weak_ciphers

  /SP/services/https
    Properties:
        weak_ciphers = disabled
```

It is recommended that this capability be disabled. To disable the use of weak and medium strength ciphers, use the command:

```
-> set /SP/services/https weak_ciphers=disabled
```

Disable Unapproved SNMP Protocols

By default, only the SNMPv3 protocol is enabled for the SNMP service that is used to monitor and manage the Oracle ILOM. Customers should ensure that older versions of the SNMP protocol are disabled unless required. To determine the status of each of the SNMP protocols, use the command:

```
-> show /SP/services/snmp v1 v2c v3

  /SP/services/snmp
    Properties:
        v1 = disabled
        v2c = disabled
        v3 = enabled
```

To disable SNMPv1 and SNMPv2c, use the commands:

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

Some Oracle and third-party products are limited in their support for newer SNMP protocol versions. Refer to the product documentation associated with those components to confirm their support for specific SNMP protocol versions. Ensure that Oracle ILOM is configured to support any protocol versions required by those components.

Version 3 of the SNMP protocol introduced support for the User-based Security Model (USM). This functionality replaces the traditional SNMP community strings with actual user accounts that can be configured with specific permissions, authentication and privacy protocols, as well as passwords. By default, the Oracle ILOM does not include any USM accounts. Customers are encouraged to configure SNMPv3 USM accounts based upon their own deployment, management and monitoring requirements.

Configure SNMP Community Strings

This item is only applicable if SNMP v1 or SNMPv2c are configured for use. As a reminder, in order for SNMP to operate correctly a client and server must agree on the community string that will be used to authenticate access. Therefore, when changing SNMP community strings, be sure that the new string is configured on both the Oracle ILOM as well as any components that will attempt to connect with Oracle ILOM using the SNMP protocol.

Given that SNMP is often used to monitor the health of the device, it is important that the default SNMP community strings used by the device be replaced with customer-defined values.

To create a new SNMP community string, use the command:

```
-> create /SP/services/snmp/communities/<string> permission=<access>
```

In the above example, the value of `<string>` should be replaced with a customer-defined value that is compliant with DoD requirements regarding the composition of SNMP community strings. Similarly, the value of the `<access>` should be replaced with either `ro` or `rw` depending upon whether read-only or read-write access is intended. Once new community strings are created, the default community strings should be removed.

To remove the default SNMP community strings, use the commands:

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

To verify the SNMP community strings that are configured, use the command:

```
-> show /SP/services/snmp/communities
```

Replace Default Self-Signed Certificates

The Oracle ILOM leverages self-signed SSL certificates to enable the "out of the box" use of the SSL/TLS protocols. Whenever possible, self-signed SSL certificates should be replaced with certificates that are approved for use in the customer's environment and signed by a recognized certificate authority. To determine if the Oracle ILOM is using its default self-signed SSL certificate, use the command:

```
-> show /SP/services/https/ssl cert_status

  /SP/services/https/ssl
    Properties:
        cert_status = Using Default (No custom certificate or private key loaded)
```

To install a customer SSL certificate use the following commands:

```
-> set /SP/services/https/ssl/custom_cert load_uri=<URI_method>
-> set /SP/services/https/ssl/custom_key load_uri=<URI_method>
```

The Oracle ILOM supports a variety of methods that can be used to access the SSL certificate and private key including HTTPS, HTTP, SCP, FTP, TFTP as well as pasting the information directly into a web browser interface. For more information, see the Oracle ILOM Configuration and Maintenance Guide.

Configure Administrative Interface Inactivity Timeout (Browser)

The Oracle ILOM supports the ability to disconnect and log out administrative sessions that have been inactive for more than some pre-defined number of minutes. By default, the browser interface will timeout a session after 15 minutes.

To check the inactivity timeout parameter associated with the HTTPS service, use the command:

```
-> show /SP/services/https sessiontimeout

  /SP/services/https
    Properties:
        sessiontimeout = 15
```

To set the inactivity timeout parameter to a customer-defined value (<n> in minutes), use the command:

```
-> set /SP/services/https sessiontimeout=<n>
```

Similarly, to check the inactivity timeout parameter associated with the HTTP service, use the command:

```
-> show /SP/services/http sessiontimeout

  /SP/services/http
    Properties:
        sessiontimeout = 15
```

To set the inactivity timeout parameter to a customer-defined value (<n> in minutes), use the command:

```
-> set /SP/services/http sessiontimeout=<n>
```

Configure Administrative Interface Inactivity Timeout (CLI)

The Oracle ILOM supports the ability to disconnect and log out administrative sessions that have been inactive for more than some pre-defined number of minutes. By default, the Secure Shell command line interface (CLI) will timeout a session after 15 minutes.

To check the inactivity timeout parameter associated with the command line interface, use the command:

```
-> show /SP/cli timeout

  /SP/cli
    Properties:
        timeout = 15
```

To set the inactivity timeout parameter to a customer-defined value (<n> in minutes), use the command:

```
-> set /SP/cli timeout=<n>
```

Configure Login Warning Banners

The Oracle ILOM supports the ability to display customer-specific messages both before and after an administrator has connected to the device. The Oracle ILOM connect message is displayed prior to authentication, whereas the login message is displayed after authentication. Optionally, a customer can configure the Oracle ILOM to require acceptance of the login message prior to being granted access to Oracle ILOM functions. The connect and login messages as well as the optional acceptance requirement are implemented by both the browser and command line access interfaces.

To determine if connect and login messages are configured, use the command:

```
-> show /SP/preferences/banner connect_message login_message

  /SP/preferenes/banner
    Properties:
        connect_message = (none)
        login_message = (none)
```

To set a connect or login message, use commands similar to the following:

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

Note that the Oracle ILOM supports connect and login messages up to a maximum of 1,000 characters. An enhancement request has been recorded to increase this limit to be more inclusive of larger banner messages used by the U.S. Federal Government. Interested customers should file a service request regarding RFE 17495689.

Once a login message has been configured, to determine if login message acceptance is enabled, use the command:

```
-> show /SP/preferences/banner login_message_acceptance

  /SP/preferenes/banner
    Properties:
        login_message_acceptance = disabled
```

To enforce acceptance of the login message, use the command:

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

Warning: Requiring login message acceptance may inhibit the correct operation of automated management processes that use Secure Shell as they may not be able or configured to respond to the acceptance request. As a result, such connections may hang or time out as the Oracle ILOM will not permit use of the command line interface until the message acceptance requirement has been satisfied.

Management Network Recommendations

In addition to the above security hardening procedures, the Oracle Exadata Storage server is intended to be deployed on a dedicated, isolated management network. This will help to shield the Oracle Exadata Storage server from unauthorized or unintended network traffic. Access to this management network should be strictly controlled with access granted only to those administrators requiring this level of access.

Commonly Reported Security Findings and Recommendations

The following issues may be reported by some commercial and/or open-source vulnerability scanners when configured to assess the security posture of the Oracle ILOM. This section is intended to provide information on commonly reported findings as well as specific technical recommendations to respond to these findings.

ORACLE ILOM SECURITY FINDINGS AND RECOMMENDATIONS

Item	CVE	CVSS	Description and Recommendation
SSL Self-Signed Certificate, SSL Certificate Cannot Be Trusted	N/A	6.4 (Medium)	These two issues were reported on all Oracle ILOM 3.2 and Oracle ILOM 3.1 versions. By default, these components are shipped with a self-signed certificate used for SSL/TLS communications. To mitigate this issue, replace the self-signed certificate with one that has been signed by a recognized certificate authority, per the instructions above.
SSL RC4 Cipher Suites Supported	CVE-2013-2566	2.6 (Low)	This issue was reported on Oracle ILOM 3.1 when the Remote KVMS service was enabled and running on TCP/5555. To mitigate this issue, disable the KVMS service as noted earlier in this document. This issue, recorded as Bug ID #16802593, has been corrected in newer versions of the ILOM software. Customers interested in this functionality should open Oracle Service Requests against the Oracle Exadata Storage Servers and Oracle ZFS Storage Appliance to adopt newer versions of the Oracle ILOM software. Note that when one of these components is used as part of an integrated Oracle Engineered System, the newer software version must first be certified and supported on that overall platform before the individual component can be upgraded.
SSL Medium Strength Cipher Suites Supported	N/A	4.3 (Medium)	This issue was reported on Oracle ILOM 3.1 when the Remote KVMS service was enabled and running on TCP/5555. To mitigate this issue, disable the KVMS service as noted earlier in this document. This issue, recorded as Bug ID #16802593, has been corrected in newer versions of the ILOM software. Customers interested in this functionality should open Oracle Service Requests against the Oracle Exadata Storage Servers and Oracle ZFS Storage Appliance to adopt newer versions of the Oracle ILOM software. Note that when one of these components is used as part of an integrated Oracle Engineered System, the newer software version must first be certified and supported on that overall platform before the individual component can be upgraded.

Item	CVE	CVSS	Description and Recommendation
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	CVE-2009-3555	5.8 (Medium)	This issue was reported on Oracle ILOM 3.1 for the HTTPS browser interface (TCP/443) and the KVMS service (TCP/5556). To mitigate this issue, disable the browser interface (HTTPS) as well as the KVMS service. This issue, recorded as Bug ID #16462493, has been corrected in newer versions of the ILOM software. Customers interested in this functionality should open Oracle Service Requests against the Oracle Exadata Storage Servers and Oracle ZFS Storage Appliance to adopt newer versions of the Oracle ILOM software. Note that when one of these components is used as part of an integrated Oracle Engineered System, the newer software version must first be certified and supported on that overall platform before the individual component can be upgraded.
NTP monlist Command Enabled	CVE-2013-5211	5.0 (Medium)	This issue was reported for the embedded NTP service running on UDP/123 across all Oracle ILOM 3.2 and Oracle ILOM 3.1 versions. There is currently no method available today to configure or disable specific functionality used by the embedded NTP implementation on this product. This issue, recorded as Bug ID #18640436, has been corrected in newer versions of the ILOM software. Customers interested in this functionality should open Oracle Service Requests against the Oracle SPARC T5-8, Oracle M6-32, and Exadata Storage Servers as well as the Oracle ZFS Storage Appliance to adopt newer versions of the Oracle ILOM software.
SSH Weak MAC Algorithms Enabled	N/A	2.6 (Low)	This issue was reported for the embedded Secure Shell service running on TCP/22 across all Oracle ILOM 3.2 and Oracle ILOM 3.1 versions. There is currently no method available today to configure or disable specific HMAC algorithms used by the embedded SSH implementation on this product. A product enhancement request has been filed to add this functionality. Interested customers can track this as RFE ID #18042406.
SSH Server CBC Mode Ciphers Enabled	CVE-2008-5161	2.6 (Low)	This issue was reported for the embedded Secure Shell service running on TCP/22 across all Oracle ILOM 3.2 and Oracle ILOM 3.1 versions. There is currently no method available today to configure or disable specific cipher algorithms used by the embedded SSH implementation on this product. A product enhancement request has been filed to add this functionality. Interested customers can track this as RFE ID #18042307. CVE-2008-5161 has already been addressed by and is not applicable to the SSH service used by Oracle ILOM 3.1 and newer.

Additional Information

For more information describing the features and capabilities of the Oracle Integrated Lights Out Manager as well as detailed technical instructions for the installation, configuration and management of this product, refer to the Oracle product documentation at:

» Oracle Integrated Lights Out Manager (ILOM) 3.2 Product Documentation
http://docs.oracle.com/cd/E37444_01/

» Oracle Integrated Lights Out Manager (ILOM) 3.1 Product Documentation
http://docs.oracle.com/cd/E24707_01/

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Hardware and Software, Engineered to Work Together

Oracle Integrated Lights Out Manager Security Configuration Supplement for the United States Department of Defense
October 2014
Author: Glenn Brunette
Contributing Authors: