| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Imagemagick** | | | | | |
| ***Imagemagick*** | | | | | |
| DoS | 07-10-2018 | **4.3** | In ImageMagick 7.0.8-13 Q16, there is a heap-based buffer over-read in the EncodeImage function of coders/pict.c, which allows attackers to cause a denial of service via a crafted SVG image file. **CVE-ID:CVE-2018-18025** | https://github.com/ImageMagick/ImageMagick/issues/1335 | A-Ima-Image/01-11-18/1 |
| DoS | 07-10-2018 | 4.3 | In ImageMagick 7.0.8-13 Q16, there is a heap-based buffer over-read in the SVGStripString function of coders/svg.c, which allows attackers to cause a denial of service via a crafted SVG image file. **CVE-ID:CVE-2018-18023** | https://github.com/ImageMagick/ImageMagick/issues/1336 | A-Ima-Image/01-11-18/2 |
| DoS | 07-10-2018 | 4.3 | In ImageMagick 7.0.8-13 Q16, there is an infinite loop in the ReadBMPImage function of the coders/bmp.c file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file. **CVE-ID:CVE-2018-18024** | https://github.com/ImageMagick/ImageMagick/issues/1337 | A-Ima-Image/01-11-18/3 |
| NA | 03-10-2018 | 4.3 | ImageMagick 7.0.7-28 has a memory leak vulnerability in ReadBGRImage in coders/bgr.c. **CVE-ID:CVE-2018-17967** | https://github.com/ImageMagick/ImageMagick/issues/1051,https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-17967 | A-Ima-Image/01-11-18/4 |
| NA | 03-10-2018 | 4.3 | ImageMagick 7.0.7-28 has a memory leak vulnerability in WritePDBImage in coders/pdb.c. **CVE-ID:CVE-2018-17966** | https://github.com/ImageMagick/ImageMagick/issues/1050,https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-17966 | A-Ima-Image/01-11-18/5 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NA | 03-10-2018 | 4.3 | ImageMagick 7.0.7-28 has a memory leak vulnerability in WriteSGIImage in coders/sgi.c. CVE-**ID:CVE-2018-17965** | https://github.com/ImageMagick/ImageMagick/issues/1052,https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-17965 | A-Ima-Image/01-11-18/6 |
| NA | 05-10-2018 | 4.3 | ImageMagick 7.0.7-28 has a memory leak vulnerability in WritePCXImage in coders/pcx.c. **CVE-ID:CVE-2018-18016** | https://github.com/ImageMagick/ImageMagick/issues/1049,https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-18016 | A-Ima-Image/01-11-18/7 |
| NA | 20-10-2018 | 4.3 | There is a memory leak in the function WriteMSLImage of coders/msl.c in ImageMagick 7.0.8-13 Q16**. CVE-ID:CVE-2018-18544** | https://github.com/ImageMagick/ImageMagick/issues/1360 | A-Ima-Image/01-11-18/8 |
| **Oracle** | | | | | |
| ***Application Management Pack*** | | | | | |
| NA | 16-10-2018 | 5 | Vulnerability in the Application Management Pack for Oracle E-Business Suite component of Oracle E-Business Suite (subcomponent: User Monitoring). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Application Management Pack for Oracle E-Business Suite. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Application Management Pack for Oracle E-Business Suite accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Appli/01-11-18/9 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **3167** | | |
| ***Application Object Library*** | | | | | |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Attachments / File Upload). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-3244** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Appli/01-11-18/10 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Attachments / File Upload). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Appli/01-11-18/11 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | or complete access to all Oracle Application Object Library accessible data as well as unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3138** | | |
| ***Applications Framework*** | | | | | |
| NA | 16-10-2018 | 4 | Vulnerability in the Oracle Applications Framework component of Oracle E-Business Suite (subcomponent: REST Services). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2971** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Appli/01-11-18/12 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Applications Framework component of Oracle E-Business Suite (subcomponent: None). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5 and 12.2.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Appli/01-11-18/13 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3243** | | |
| **Applications Manager** | | | | | |
| Gain Information | 16-10-2018 | 5 | Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite (subcomponent: Support Cart). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Manager accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3237** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Appli/01-11-18/14 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite | http://www.oracle.com/technetwork/security- | A-Ora-Appli/01-11-18/15 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (subcomponent: None). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3235** | advisory/cpuoct2018-4428296.html | |
| **Business Intelligence** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: Analytics Server). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Busin/01-11-18/16 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3204** | | |
| ***Connector/j*** | | | | | |
| NA | 16-10-2018 | 6.5 | Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3258** | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Conne/01-11-18/17 |
| ***Customer Interaction History*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Customer Interaction History component of Oracle E-Business Suite (subcomponent: Outcome-Result). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Custo/01-11-18/18 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Customer Interaction History accessible data as well as unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3189** | | |
| ***Database Server*** | | | | | |
| *NA* | *16-10-2018* | *7.5* | Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3259** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Datab/01-11-18/19 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ***Demantra Demand Management*** | | | | | |
| NA | 16-10-2018 | 4.3 | Vulnerability in the Oracle Demantra Demand Management component of Oracle Supply Chain Products Suite (subcomponent: Product Security). Supported versions that are affected are 7.3.5 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Demantra Demand Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Demantra Demand Management accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-3127** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Deman/01-11-18/20 |
| ***E-business Intelligence*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle E-Business Intelligence component of Oracle E-Business Suite (subcomponent: Overview Page/Report Rendering). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle E-Business Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-E-bus/01-11-18/21 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | critical data or complete access to all Oracle E-Business Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle E-Business Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3190** | | |
| **Email Center** | | | | | |
| NA | 16-10-2018 | 4.3 | Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE-ID:CVE-2018-3256** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Email/01-11-18/22 |
| ***Endeca Information Discovery Integrator*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Endeca Information Discovery Integrator component of Oracle Fusion Middleware (subcomponent: | http://www.oracle.com/technetwork/security-advisory/cpuoct2 | A-Ora-Endec/01-11-18/23 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Integrator ETL). Supported versions that are affected are 3.1.0 and 3.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Endeca Information Discovery Integrator. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Endeca Information Discovery Integrator accessible data as well as unauthorized read access to a subset of Oracle Endeca Information Discovery Integrator accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-3215** | 018-4428296.html | |
| ***Glassfish Server*** | | | | | |
| DoS | 16-10-2018 | 6.8 | Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware (subcomponent: Java Server Faces). The supported version that is affected is 3.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GlassFish Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GlassFish Server accessible data as well as unauthorized access to critical data or complete access to | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Glass/01-11-18/24 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | all Oracle GlassFish Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GlassFish Server. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L). **CVE-ID:CVE-2018-2911** | | |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware (subcomponent: Administration). The supported version that is affected is 3.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GlassFish Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GlassFish Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3152** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Glass/01-11-18/25 |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware (subcomponent: Java Server Faces). The supported version that is affected is 3.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GlassFish Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GlassFish Server accessible data. CVSS 3.0 Base Score 5.3 | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Glass/01-11-18/26 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N**). CVE-ID:CVE-2018-3210** | | |
| ***Goldengate*** | | | | | |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle GoldenGate component of Oracle GoldenGate (subcomponent: Manager). Supported versions that are affected are 12.1.2.1.0, 12.2.0.2.0 and 12.3.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle GoldenGate. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GoldenGate. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-2912** | https://www.tenable.com/security/research/tra-2018-31 | A-Ora-Golde/01-11-18/27 |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle GoldenGate component of Oracle GoldenGate (subcomponent: Manager). Supported versions that are affected are 12.1.2.1.0, 12.2.0.2.0 and 12.3.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle GoldenGate. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GoldenGate. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-** | https://www.tenable.com/security/research/tra-2018-31 | A-Ora-Golde/01-11-18/28 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **2914** | | |
| Overflow | 16-10-2018 | 7.5 | Vulnerability in the Oracle GoldenGate component of Oracle GoldenGate (subcomponent: Monitoring Manager). Supported versions that are affected are 12.1.2.1.0, 12.2.0.2.0 and 12.3.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle GoldenGate. While the vulnerability is in Oracle GoldenGate, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle GoldenGate. Note: For Linux and Windows platforms, the CVSS score is 9.0 with Access Complexity as High. For all other platforms, the cvss score is 10.0. CVSS 3.0 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2913** | https://www.tenable.com/security/research/tra-2018-31 | A-Ora-Golde/01-11-18/29 |
| ***Hospitality Cruise Fleet Management*** | | | | | |
| DoS | 16-10-2018 | 6.4 | Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: Emergency Response System). The supported version that is affected is 9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Cruise Fleet Management accessible data | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hospi/01-11-18/30 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Cruise Fleet Management. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L). **CVE-ID:CVE-2018-3163** | | |
| NA | 16-10-2018 | 3.6 | Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: Sender and Receiver). The supported version that is affected is 9.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Cruise Fleet Management executes to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Fleet Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Fleet Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE-ID:CVE-2018-3159** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hospi/01-11-18/31 |
| NA | 16-10-2018 | 4 | Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: Emergency Response System). The supported version that is affected is 9.0. Easily exploitable vulnerability | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hospi/01-11-18/32 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Cruise Fleet Management accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N). **CVE-ID:CVE-2018-3166** | | |
| NA | 16-10-2018 | 5.5 | Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: Emergency Response System). The supported version that is affected is 9.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Fleet Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Fleet Management accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE-ID:CVE-2018-3158** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hospi/01-11-18/33 |
| ***Hospitality Cruise Shipboard Property Management System*** | | | | | |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System | http://www.oracle.com/technetwork/security- | A-Ora-Hospi/01-11-18/34 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | component of Oracle Hospitality Applications (subcomponent: OHC Admin, OHC Management). The supported version that is affected is 8.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hospitality Cruise Shipboard Property Management System executes to compromise Oracle Hospitality Cruise Shipboard Property Management System. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Cruise Shipboard Property Management System, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Cruise Shipboard Property Management System. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3160** | advisory/cpuoct2018-4428296.html | |
| ***Hospitality Gift And Loyalty*** | | | | | |
| NA | 16-10-2018 | 3.6 | Vulnerability in the Oracle Hospitality Gift and Loyalty component of Oracle Food and Beverage Applications. The supported version that is affected is 9.0. Easily exploitable vulnerability allows low privileged attacker having Report privilege with logon to the infrastructure where Oracle Hospitality Gift and Loyalty executes to compromise Oracle Hospitality Gift and Loyalty. Successful attacks of this vulnerability can result in | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hospi/01-11-18/35 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthorized access to critical data or complete access to all Oracle Hospitality Gift and Loyalty accessible data as well as unauthorized update, insert, or delete access to some of Oracle Hospitality Gift and Loyalty accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE-ID:CVE-2018-3131** | | |
| **Hospitality Reporting And Analytics** | | | | | |
| NA | 16-10-2018 | 5.5 | Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.0. Easily exploitable vulnerability allows low privileged attacker having Report privilege with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion, or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3128** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hospi/01-11-18/36 |
| ***Hyperion*** | | | | | |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NA | 16-10-2018 | 4 | Vulnerability in the Hyperion Essbase Administration Services component of Oracle Hyperion (subcomponent: EAS Console). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. While the vulnerability is in Hyperion Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Essbase Administration Services accessible data. CVSS 3.0 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE-ID:CVE-2018-3142** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hyper/01-11-18/43 |
| NA | 16-10-2018 | 5 | Vulnerability in the Hyperion Essbase Administration Services component of Oracle Hyperion (subcomponent: EAS Console). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. While the vulnerability is in Hyperion Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Essbase | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hyper/01-11-18/44 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Administration Services accessible data. CVSS 3.0 Base Score 5.8 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N). **CVE-ID:CVE-2018-3141** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Hyperion Essbase Administration Services component of Oracle Hyperion (subcomponent: EAS Console). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Essbase Administration Services accessible data as well as unauthorized read access to a subset of Hyperion Essbase Administration Services accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3140** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hyper/01-11-18/45 |
| ***Hyperion Common Events*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Hyperion Common Events component of Oracle Hyperion (subcomponent: User Interface). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hyper/01-11-18/38 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allows unauthenticated attacker with network access via HTTP to compromise Hyperion Common Events. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Common Events, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Common Events accessible data as well as unauthorized read access to a subset of Hyperion Common Events accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3175** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Hyperion Common Events component of Oracle Hyperion (subcomponent: User Interface). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Common Events. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Common Events, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Common Events accessible data as well as unauthorized read access to a subset | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hyper/01-11-18/39 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of Hyperion Common Events accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3176** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Hyperion Common Events component of Oracle Hyperion (subcomponent: User Interface). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Common Events. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Common Events, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Common Events accessible data as well as unauthorized read access to a subset of Hyperion Common Events accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3177** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hyper/01-11-18/40 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Hyperion Common Events component of Oracle Hyperion (subcomponent: User Interface). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hyper/01-11-18/41 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | compromise Hyperion Common Events. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Common Events, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Common Events accessible data as well as unauthorized read access to a subset of Hyperion Common Events accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3178** | | |
| ***Hyperion Data Relationship Management*** | | | | | |
| NA | 16-10-2018 | 4 | Vulnerability in the Hyperion Data Relationship Management component of Oracle Hyperion (subcomponent: Access and Security). The supported version that is affected is 11.1.2.4.345. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hyperion Data Relationship Management. While the vulnerability is in Hyperion Data Relationship Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Data Relationship Management accessible data. CVSS 3.0 Base Score 7.7 (Confidentiality impacts). CVSS Vector: | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Hyper/01-11-18/42 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE-ID:CVE-2018-3208** | | |
| ***Identity Analytics*** | | | | | |
| NA | 16-10-2018 | 5.5 | Vulnerability in the Oracle Identity Analytics component of Oracle Fusion Middleware (subcomponent: Core Components). The supported version that is affected is 11.1.1.5.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Identity Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Analytics accessible data as well as unauthorized read access to a subset of Oracle Identity Analytics accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N). **CVE-ID:CVE-2018-3168** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Ident/01-11-18/46 |
| **Identity Manager** | | | | | |
| DoS | 16-10-2018 | 6.4 | Vulnerability in the Oracle Identity Manager component of Oracle Fusion Middleware (subcomponent: Advanced Console). Supported versions that are affected are 11.1.2.3.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager. While the vulnerability is in Oracle Identity Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Ident/01-11-18/47 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthorized read access to a subset of Oracle Identity Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Identity Manager. CVSS 3.0 Base Score 7.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L). **CVE-ID:CVE-2018-3179** | | |
| ***Ilearning*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle iLearning component of Oracle iLearning (subcomponent: Learner Administration). Supported versions that are affected are 6.1 and 6.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iLearning. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iLearning, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iLearning accessible data as well as unauthorized update, insert or delete access to some of Oracle iLearning accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3146** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Ilear/01-11-18/48 |
| ***Iprocurement*** | | | | | |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle iProcurement component of Oracle E-Business Suite (subcomponent: E- | http://www.oracle.com/technetwork/security- | A-Ora-Iproc/01-11-18/49 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Content Manager Catalog). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iProcurement. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iProcurement accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3151** | advisory/cpuoct2018-4428296.html | |
| ***Istore*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Web interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Istor/01-11-18/50 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3188** | | |
| ***JDK,JRE*** | | | | | |
| Execute Code | 16-10-2018 | 3.3 | Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Serviceability). Supported versions that are affected are Java SE: 8u182 and 11; Java SE Embedded: 8u181. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Java SE, Java SE Embedded executes to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by an administrator). This vulnerability can only be exploited when Java Usage Tracker functionality is being used. CVSS 3.0 Base Score 6.6 | https://access.redhat.com/errata/RHSA-2018:3002,https://security.netapp.com/advisory/ntap-20181018-0001/,https://access.redhat.com/errata/RHSA-2018:3003 | A-Ora-JDK,J/01-11-18/51 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3211** | | |
| NA | 16-10-2018 | 4.3 | Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Sound). The supported version that is affected is Java SE: 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3157** | https://security.netapp.com/advisory/ntap-20181018-0001/ | A-Ora-JDK,J/01-11-18/52 |
| NA | 16-10-2018 | 4.3 | Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Utility). The supported version that is affected is Java SE: 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete | https://security.netapp.com/advisory/ntap-20181018-0001/,https://usn.ubuntu.com/3804-1/ | A-Ora-JDK,J/01-11-18/53 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | access to some of Java SE accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-3150** | | |
| NA | 16-10-2018 | 5.1 | Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). The supported version that is affected is Java SE: 8u182. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by an | https://security.netapp.com/advisory/ntap-20181018-0001/,https://access.redhat.com/errata/RHSA-2018:3003,https://access.redhat.com/errata/RHSA-2018:3002 | A-Ora-JDK,J/01-11-18/54 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3209** | | |
| ***Marketing*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3242** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Marke/01-11-18/55 |
| ***Micros Retail-j*** | | | | | |
| NA | 16-10-2018 | 5 | Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Internal Operations). The supported version that is affected is 12.1.2. Easily exploitable vulnerability | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Micro/01-11-18/56 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allows unauthenticated attacker with network access via HTTP to compromise MICROS Retail-J. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MICROS Retail-J accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2889** | | |
| NA | 16-10-2018 | 6.4 | Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Back Office). Supported versions that are affected are 13.0.0 and 12.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MICROS Retail-J. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MICROS Retail-J accessible data as well as unauthorized read access to a subset of MICROS Retail-J accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-2887** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Micro/01-11-18/57 |
| ***Mysql*** | | | | | |
| NA | 16-10-2018 | 3.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/58 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3284** | | |
| NA | 16-10-2018 | 3.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Logging). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3283** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/59 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/60 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S: U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3143** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S: U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3156** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/61 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S: | https://usn.ubuntu.com/3799-1/,https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/62 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3251** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3162** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/63 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3173** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/64 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported | https://security.netapp.com/advisory/ntap- | A-Ora-Mysql/01-11-18/65 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3200** | 20181018-0002/,https://usn.ubuntu.com/3799-1/ | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3277** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/66 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/67 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3170** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3182** | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/68 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/69 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3212** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3276** | https://usn.ubuntu.com/3799-1/,https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/70 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S: | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/71 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3186** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S: U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3137** | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/72 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S: U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3203** | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/73 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). | https://usn.ubuntu.com/3799-2/,https://usn.ub | A-Ora-Mysql/01-11-18/74 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3133** | untu.com/3799-1/,https://security.netapp.com/advisory/ntap-20181018-0002/ | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE-ID:CVE-2018-3155** | https://usn.ubuntu.com/3799-1/,https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/75 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/76 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3145** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3161** | https://usn.ubuntu.com/3799-1/,https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/77 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: RBR). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to | https://usn.ubuntu.com/3799-1/,https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/78 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3278** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-3286** | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/79 |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/80 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3279** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3282** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-2/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/81 |
| NA | 16-10-2018 | 4.3 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/82 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **3144** | | |
| NA | 16-10-2018 | 4.9 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE-ID:CVE-2018-3171** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/83 |
| NA | 16-10-2018 | 5.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S: | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/84 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | U/C:N/I:L/A:H). **CVE-ID:CVE-2018-3185** | | |
| NA | 16-10-2018 | 5.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S: U/C:N/I:L/A:H). **CVE-ID:CVE-2018-3195** | https://security.netapp.com/advisory/ntap-20181018-0002/ | A-Ora-Mysql/01-11-18/85 |
| NA | 16-10-2018 | 5.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Merge). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/86 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE-ID:CVE-2018-3247** | | |
| NA | 16-10-2018 | 5.5 | Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE-ID:CVE-2018-3187** | https://security.netapp.com/advisory/ntap-20181018-0002/,https://usn.ubuntu.com/3799-1/ | A-Ora-Mysql/01-11-18/87 |
| ***Outside In Technology*** | | | | | |
| DoS | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/88 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3219** | | |
| DoS | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/89 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3220** | | |
| NA | 16-10-2018 | 4.3 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 4.3 (Confidentiality | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/90 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3147** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3221** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/91 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: | http://www.oracle.com/technetwork/security- | A-Ora-Outsi/01-11-18/92 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3222** | advisory/cpuoct2018-4428296.html | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/93 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3223** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/94 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3224** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/95 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3225** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/96 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3226** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3227** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/97 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle | http://www.oracle.com/technetwor | A-Ora-Outsi/01- |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3228** | k/security-advisory/cpuoct2018-4428296.html | 11-18/98 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/99 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3229** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/100 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3230** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/101 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3231** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/102 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3232** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3233** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/103 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3234** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/104 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/105 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H). **CVE-ID:CVE-2018-3302** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/106 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE-ID:CVE-2018-3217** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data. Note: Outside In | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Outsi/01-11-18/107 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE-ID:CVE-2018-3218** | | |
| ***Partner Management*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Partner Management component of Oracle E-Business Suite (subcomponent: Partner Dashboard). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Partner Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Partner Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Partner Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Partn/01-11-18/108 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3196** | | |
| ***Peoplesoft Enterprise Interaction Hub*** | | | | | |
| NA | 16-10-2018 | 5.5 | Vulnerability in the PeopleSoft Enterprise Interaction Hub component of Oracle PeopleSoft Products (subcomponent: Application Portal). The supported version that is affected is 9.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise Interaction Hub. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise Interaction Hub accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise Interaction Hub accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-3130** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/109 |
| **Peoplesoft Enterprise Peopletools** | | | | | |
| NA | 16-10-2018 | 4.3 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/110 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-3129** | | |
| NA | 16-10-2018 | 4.3 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE-ID:CVE-2018-3135** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/111 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NA | 16-10-2018 | 4.3 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Stylesheet). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE-ID:CVE-2018-3262** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/112 |
| NA | 16-10-2018 | 5 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Integration Broker). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/113 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3261** | | |
| NA | 16-10-2018 | 5 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Integration Broker). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3239** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/114 |
| NA | 16-10-2018 | 5 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Performance Monitor). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3202** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/115 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NA | 16-10-2018 | 5 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3198** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/116 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Activity Guide). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/117 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3193** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Activity Guide). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3194** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/118 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Elastic Search). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/119 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3164** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Core). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/120 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3255** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3153** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/121 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products | http://www.oracle.com/technetwork/security- | A-Ora-Peopl/01-11-18/122 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3257** | advisory/cpuoct2018-4428296.html | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/123 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3301** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/124 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **3154** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3206** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/125 |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/126 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3207** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Rich Text Editor). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/127 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3132** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Workflow). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3205** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/128 |
| NA | 16-10-2018 | 6.5 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Query). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows high privileged attacker with network access via | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/129 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3192** | | |
| NA | 16-10-2018 | 6.5 | Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: SQR). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3165** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Peopl/01-11-18/130 |
| ***Primavera P6 Enterprise Project Portfolio Management*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.1, 15.2, 16.1, 16.2, 17.7 - 17.12 and 18.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Prima/01-11-18/131 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3241** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.1, 15.2, 16.1, 16.2, 17.7 - 17.12 and 18.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Prima/01-11-18/132 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3281** | | |
| **Primavera Unifier** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Primavera Unifier component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 15.1, 15.2, 16.1, 16.2, 17.1-17.12 and 18.1-18.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Unifier. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Unifier, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Unifier accessible data as well as unauthorized read access to a subset of Primavera Unifier accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3148** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Prima/01-11-18/133 |
| ***Retail Open Commerce Platform*** | | | | | |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NA | 16-10-2018 | 4.9 | Vulnerability in the Oracle Retail Open Commerce Platform component of Oracle Retail Applications (subcomponent: Integrations). Supported versions that are affected are 6.0, 6.0.1 and 5.3. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Open Commerce Platform. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Retail Open Commerce Platform accessible data as well as unauthorized access to critical data or complete access to all Oracle Retail Open Commerce Platform accessible data. CVSS 3.0 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3122** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Retai/01-11-18/134 |
| ***Retail Sales Audit*** | | | | | |
| DoS | 16-10-2018 | 6 | Vulnerability in the Oracle Retail Sales Audit component of Oracle Retail Applications (subcomponent: Operational Insights). Supported versions that are affected are 15.0 and 16.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Sales Audit. While the vulnerability is in Oracle Retail Sales Audit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Sales Audit accessible data as | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Retai/01-11-18/135 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | well as unauthorized update, insert or delete access to some of Oracle Retail Sales Audit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Sales Audit. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L). **CVE-ID:CVE-2018-3115** | | |
| ***Retail Xstore Point Of Service*** | | | | | |
| NA | 16-10-2018 | 6 | Vulnerability in the Oracle Retail Xstore Point of Service component of Oracle Retail Applications (subcomponent: Xenvironment). Supported versions that are affected are 15.0.2, 16.0.4 and 17.0.2. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Retail Xstore Point of Service. Successful attacks of this vulnerability can result in takeover of Oracle Retail Xstore Point of Service. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3126** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Retai/01-11-18/136 |
| ***Siebel Ui Framework*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 18.7, 18.8 and 18.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Siebe/01-11-18/137 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interaction from a person other than the attacker and while the vulnerability is in Siebel UI Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized read access to a subset of Siebel UI Framework accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3059** | | |
| ***Text*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Text. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Text, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Text as well as unauthorized update, insert or delete access to some of Oracle Text accessible data. CVSS 3.0 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Text/01-11-18/138 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:H). **CVE-ID:CVE-2018-3299** | | |
| ***Trade Management*** | | | | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3011** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Trade/01-11-18/139 |
| ***User Management*** | | | | | |
| NA | 16-10-2018 | 5.5 | Vulnerability in the Oracle User Management component of Oracle E-Business Suite (subcomponent: Reports). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows high privileged attacker with network | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-User/01-11-18/140 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle User Management accessible data as well as unauthorized access to critical data or complete access to all Oracle User Management accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3236** | | |
| ***Virtual Directory*** | | | | | |
| DoS | 16-10-2018 | 6 | Vulnerability in the Oracle Virtual Directory component of Oracle Fusion Middleware (subcomponent: Virtual Directory Manager). Supported versions that are affected are 11.1.1.7.0 and 11.1.1.9.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Virtual Directory. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Virtual Directory accessible data as well as unauthorized read access to a subset of Oracle Virtual Directory accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Virtual Directory. CVSS 3.0 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3253** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Virtu/01-11-18/141 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ***Vm Virtualbox*** | | | | | |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2909** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/142 |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/143 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3287** | | |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3288** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/144 |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/145 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3289** | | |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3290** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/146 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3291** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/147 |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/148 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3292** | | |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3293** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/149 |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/150 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3295** | | |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3296** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/151 |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is | http://www.oracle.com/technetwork/security-advisory/cpuoct2 | A-Ora-Vm/01-11-18/152 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3297** | 018-4428296.html | |
| NA | 16-10-2018 | 4.4 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/153 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3298** | | |
| NA | 16-10-2018 | 6 | Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.20. Easily exploitable vulnerability allows low privileged attacker with network access via VRDP to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3294** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Vm/01-11-18/154 |
| ***Webcenter Portal*** | | | | | |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle WebCenter Portal component of Oracle Fusion Middleware (subcomponent: WebCenter Spaces Application). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Portal accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Webce/01-11-18/155 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3254** | | |
| ***Webcenter Sites*** | | | | | |
| NA | 16-10-2018 | 4.9 | Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 11.1.1.8.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 6.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3238** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Webce/01-11-18/156 |
| ***Weblogic Server*** | | | | | |
| Gain Information | 16-10-2018 | 4 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Console). Supported versions that are affected are 10.3.6.0 and 12.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Weblo/01-11-18/157 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2902** | | |
| NA | 16-10-2018 | 4 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). The supported version that is affected is 10.3.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3249** | NA | A-Ora-Weblo/01-11-18/158 |
| NA | 16-10-2018 | 4.3 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). The supported version that is affected is 10.3.6.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful | NA | A-Ora-Weblo/01-11-18/159 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3248** | | |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Docker Images). The supported version that is affected is prior to Docker 12.2.1.3.20180913. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3213** | https://www.tenable.com/security/research/tra-2018-32 | A-Ora-Weblo/01-11-18/160 |
| NA | 16-10-2018 | 5 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Weblo/01-11-18/161 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3246** | | |
| NA | 16-10-2018 | 5.8 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). The supported version that is affected is 10.3.6.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3250** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Weblo/01-11-18/162 |
| NA | 16-10-2018 | 7.5 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Weblo/01-11-18/163 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3191** | | |
| NA | 16-10-2018 | 7.5 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3245** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Weblo/01-11-18/164 |
| NA | 16-10-2018 | 7.5 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Weblo/01-11-18/165 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3252** | | |
| NA | 16-10-2018 | 7.5 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). The supported version that is affected is 12.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3197** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Weblo/01-11-18/166 |
| NA | 16-10-2018 | 7.5 | Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). The supported version that is affected is 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-3201** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | A-Ora-Weblo/01-11-18/167 |
| **Prayer Project** | | | | | |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ***Prayer*** | | | | | |
| Gain Information | 25-10-2018 | 4.3 | Prayer through 1.3.5 sends a Referer header, containing a user's username, when a user clicks on a link in their email because header.t lacks a no-referrer setting. **CVE-ID:CVE-2018-18655** | https://bugs.debian.org/911842 | A-Pra-Praye/01-11-18/168 |
| **Subrion** | | | | | |
| ***CMS*** | | | | | |
| XSS | 02-10-2018 | 4.3 | _core/admin/pages/add/ in Subrion CMS 4.2.1 has XSS via the titles[en] parameter. CVE-ID:CVE-2018-15563 | https://cxsecurity.com/issue/WLB-2018090261 | A-Sub-CMS/01-11-18/169 |
| **Application,Operating System (Application,OS)** | | | | | |
| **Canonical,Debian,Libssh** | | | | | |
| ***Debian Linux,Libssh,Ubuntu Linux*** | | | | | |
| NA | 17-10-2018 | 6.4 | A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access. **CVE-ID:CVE-2018-10933** | https://www.exploit-db.com/exploits/45638/,https://www.libssh.org/security/advisories/CVE-2018-10933.txt,https://usn.ubuntu.com/3795-2/,https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0016,https://usn.ubuntu.com/3795-1/,https://www.debian.org/security/2018/dsa-4322,https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10933,https://lists.debian.org/debia | A-Can-Debia/01-11-18/170 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | n-lts-announce/2018/10/msg00010.html, https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/libssh_auth_bypass | |
| **Oracle,Redhat** | | | | | |
| ***Enterprise Linux Desktop,Enterprise Linux Server,Enterprise Linux Server Eus,Enterprise Linux Workstation,JDK,JRE*** | | | | | |
| NA | 16-10-2018 | 5.1 | Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by an | https://access.redhat.com/errata/RHSA-2018:2943, https://access.redhat.com/errata/RHSA-2018:3000, https://access.redhat.com/errata/RHSA-2018:3001, https://access.redhat.com/errata/RHSA-2018:3409, https://access.redhat.com/errata/RHSA-2018:3002, https://access.redhat.com/errata/RHSA-2018:3003, https://access.redhat.com/errata/RHSA-2018:3350, https://access.redhat.com/errata/RHSA-2018:2942, | A-Ora-Enter/01-11-18/175 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3169** | https://security.netapp.com/advisory/ntap-20181018-0001/, https://usn.ubuntu.com/3804-1/, https://www.debian.org/security/2018/dsa-4326 | |
| ***Enterprise Linux Desktop,Enterprise Linux Server,Enterprise Linux Server Eus,Enterprise Linux Workstation,JDK,JRE,Jrockit*** | | | | | |
| DoS | 16-10-2018 | 5 | Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Sound). Supported versions that are affected are Java SE: 6u201, 7u191 and 8u182; Java SE Embedded: 8u181; JRockit: R28.3.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the | https://access.redhat.com/errata/RHSA-2018:3008, https://access.redhat.com/errata/RHSA-2018:3409, https://access.redhat.com/errata/RHSA-2018:3003,https://security.netapp.com/advisory/ntap-20181018-0001/, https://access.redhat.com/errata/RHSA-2018:3350, https://access.redhat.com/errata/RHSA-2018:3007, https://access.redhat.com/errata/RHSA-2018:3002, https://access.redhat.com/errata/R | A-Ora-Enter/01-11-18/171 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-3214** | HSA-2018:2942, https://access.redhat.com/errata/RHSA-2018:2943, https://access.redhat.com/errata/RHSA-2018:3000, https://access.redhat.com/errata/RHSA-2018:3001, https://usn.ubuntu.com/3804-1/, https://www.debian.org/security/2018/dsa-4326 | |
| DoS | 16-10-2018 | 6.8 | Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, | https://access.redhat.com/errata/RHSA-2018:3350, https://access.redhat.com/errata/RHSA-2018:3409, https://security.netapp.com/advisory/ntap-20181018-0001/, https://access.redhat.com/errata/RHSA-2018:3003, https://access.redhat.com/errata/RHSA-2018:3001, https://access.redhat.com/errata/R | A-Ora-Enter/01-11-18/172 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3180** | HSA-2018:3002,<br><br>https://access.redhat.com/errata/RHSA-2018:3008,<br><br>https://access.redhat.com/errata/RHSA-2018:3007,<br><br>https://access.redhat.com/errata/RHSA-2018:3000,<br><br>https://access.redhat.com/errata/RHSA-2018:2943,<br><br>https://access.redhat.com/errata/RHSA-2018:2942,<br><br>https://usn.ubuntu.com/3804-1/,<br><br>https://www.debian.org/security/2018/dsa-4326 | |
| NA | 16-10-2018 | 5.1 | Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the | https://security.netapp.com/advisory/ntap-20181018-0001/,<br><br>https://access.redhat.com/errata/RHSA-2018:3350,<br><br>https://access.redhat.com/errata/RHSA-2018:3409,<br><br>https://access.redhat.com/errata/R | A-Ora-Enter/01-11-18/173 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3149** | HSA-2018:3008, https://access.redhat.com/errata/RHSA-2018:3007, https://access.redhat.com/errata/RHSA-2018:3003, https://access.redhat.com/errata/RHSA-2018:3002, https://access.redhat.com/errata/RHSA-2018:2942, https://access.redhat.com/errata/RHSA-2018:3001, https://access.redhat.com/errata/RHSA-2018:2943, https://access.redhat.com/errata/RHSA-2018:3000, https://usn.ubuntu.com/3804-1/, https://www.debian.org/security/2018/dsa-4326 | |
| NA | 16-10-2018 | 6.8 | Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Scripting). Supported versions that are affected are Java SE: 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated | https://usn.ubuntu.com/3804-1/, https://security.netapp.com/advisory/ntap-20181018-0001/, | A-Ora-Enter/01-11-18/174 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3183** | https://www.debian.org/security/2018/dsa-4326,<br><br>https://access.redhat.com/errata/RHSA-2018:2942<br><br>,https://access.redhat.com/errata/RHSA-2018:2943, https://access.redhat.com/errata/RHSA-2018:3003, https://access.redhat.com/errata/RHSA-2018:3002 | |
| **Operating System (OS)** | | | | | |
| **Oracle** | | | | | |
| ***Solaris*** | | | | | |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| DoS | 16-10-2018 | 3.6 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11.3. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 4.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE-ID:CVE-2018-3264** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/176 |
| DoS | 16-10-2018 | 4 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: SMB Server). The supported version that is affected is 11.3. Easily exploitable vulnerability allows low privileged attacker with network access via SMB to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-3269** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/177 |
| DoS | 16-10-2018 | 4.4 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Verified Boot). The supported version that is affected is 11.3. | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/178 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 3.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3266** | | |
| DoS | 16-10-2018 | 4.4 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Zones). The supported version that is affected is 11.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 4.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3265** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/179 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| DoS | 16-10-2018 | 5 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: RPC). Supported versions that are affected are 10 and 11.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via Portmap v3 to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-3172** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/180 |
| DoS | 16-10-2018 | 5 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: SMB Server). The supported version that is affected is 11.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via SMB to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-3268** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/181 |
| DoS | 16-10-2018 | 6.8 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Sudo). The supported version that is affected is 11.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/182 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3263** | | |
| NA | 16-10-2018 | 4.7 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel Zones). The supported version that is affected is 11.3. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. While the vulnerability is in Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE-ID:CVE-2018-3271** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/183 |
| NA | 16-10-2018 | 4.9 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel Zones Virtualized NIC Driver). The supported version that is affected is 11.3. Easily exploitable | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/184 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability allows unauthenticated attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris. CVSS 3.0 Base Score 6.2 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3272** | | |
| NA | 16-10-2018 | 5 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: LFTP). The supported version that is affected is 11.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via FTP to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Solaris accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3267** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/185 |
| NA | 16-10-2018 | 6.3 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11.3. Easily exploitable vulnerability allows low privileged attacker with network access via SMB to compromise Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/186 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris. CVSS 3.0 Base Score 5.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3274** | | |
| NA | 16-10-2018 | 8.8 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: LibKMIP). The supported version that is affected is 11.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Solaris accessible data as well as unauthorized access to critical data or complete access to all Solaris accessible data. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3275** | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/187 |
| NA | 16-10-2018 | 8.8 | Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Remote Administration Daemon (RAD)). The supported version that is affected is 11.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can | http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html | O-Ora-Solar/01-11-18/188 |

| Vulnerability Type(s) | Publish Date | CVSS | Description&CVE_ID | Reference/Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | result in unauthorized creation, deletion or modification access to critical data or all Solaris accessible data as well as unauthorized access to critical data or complete access to all Solaris accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3273** | | |