( Notice )	National Critical Information Infrastructure Protection Centre  CVE Report  CVE Scoring Scale 12, 10 and 10 of 21 Oct 2019 and 10 of 220												
	Scoring Scale			Vol. 05									
Vulnerability Type(s)	Publish Date	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID								
			Application										
Imagemagick													
<i>Imagemagick</i>													
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.co m/ImageMagick/I mageMagick/issue s/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.co m/ImageMagick/I mageMagick/issue s/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. <b>CVE-ID:CVE-2018-18024</b>	https://github.co m/ImageMagick/I mageMagick/issue s/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.co m/ImageMagick/I mageMagick/issue s/1051,https://bu gzilla.redhat.com/ show_bug.cgi?id=C VE-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. <b>CVE-ID:CVE-2018-17966</b>	https://github.co m/ImageMagick/I mageMagick/issue s/1050,https://bu gzilla.redhat.com/ show_bug.cgi?id=C VE-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	<b>Publish Date</b>	CVSS	Descrip	tion&CVE_	Referenc	e/Patch	NCIIPC ID	
NA	03-10-2018	4.3	ImageMagick 7 leak vulnerabil in coders/sgi.c 17965	ity in Write	eSGIImage	https://gi m/Imagel mageMag s/1052,ht gzilla.redl show_bug VE-2018-	Magick/I ick/issue ttps://bu nat.com/	A-Ima- Image/01- 11-18/6
NA	05-10-2018	4.3	ImageMagick 7 leak vulnerabili in coders/pcx.o 18016	ity in Write	PCXImage	https://gi m/Imagel mageMag s/1049,ht gzilla.redl show_bug VE-2018-	Magick/I ick/issue ttps://bu nat.com/ c.cgi?id=C	A-Ima- Image/01- 11-18/7
NA	20-10-2018	4.3	There is a m function W coders/msl.c ir 13 Q16. CVE-ID	riteMSLIma i ImageMag	nge of gick 7.0.8-	https://gi m/Imagel mageMag s/1360	Magick/I	A-Ima- Image/01- 11-18/8
Oracle								
	ınagement Pacl					T -		
NA	16-10-2018	5	versions that at 12.2.3, 12.2.4,	Pack for Component aite (subcoring). See affected a 12.2.5, 12 asily ellows unauth network apromise Apack for Couccessful aity can ead access to Managementess Suite 1.0 Base See impacts	Oracle E- of Oracle omponent: Supported are 12.1.3, 2.2.6 and exploitable henticated access via pplication Oracle E- attacks of result in o a subset t Pack for accessible Score 5.3 ). CVSS	http://wv e.com/teo k/security advisory/ 018-4428	chnetwor y- cpuoct2	A-Ora- Appli/01- 11-18/9
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

/ulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL
njection; XSS- Cross Site Scripting;

CV Scoring Scale (CVSS)

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			3167		
Annligation Oh	icat Library		3107		
NA 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:	e.com/technetwork/security-advisory/cpuoct2018-4428296.html	A-Ora- Appli/01- 11-18/10
NA	16-10-2018	5.8	U/C:N/I:L/A:N). CVE-ID:CVE-2018-3244  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	e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Appli/01- 11-18/11
CV Scoring Scale (C	VSS)	3-4		7-8 8-9	9-10
		Request F	orgery; Dir. TravDirectory Traversal; DoS-Den	al of Service: NA- Not Appli	cable: Sal-SOL

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	ID	Reference	e/Patch	NCIIPC ID
			App dat inso Ora acc 8.2 imp (CV	complete application Object as well as ert or deleted acts (Confident pacts).  ZSS:3.0/AV:NC:H/I:L/A:N)	ect Library unauthorize te access to ation Object CVSS 3.0 Ectality and CVSS I/AC:L/PR:N				
Applications Fi			l				T		
NA	16-10-2018	4	Apport of (sure sure sure sure sure sure sure sure	plications Fracks of the ult in unauth subset of amework accesse Score pacts).  VSS:3.0/AV:NC:L/I:N/A:N)	E-Busines E: REST Lions that and the second	component s Suite Services). The affected 4, 12.2.5, exploitable privileged access via to Oracle Successful bility cand access to oplications a. CVSS 3.0 and access to oplications and access to oplications and access to oplications and access to oplications a. CVSS 3.0 and access to oplications are access to oplications are access to oplications and access to oplications are access to oplications and access to oplications are access to oplications and access to oplications are access to opli	http://ww e.com/teo k/securit advisory/ 018-4428	chnetwor y- 'cpuoct2	A-Ora- Appli/01- 11-18/12
NA	16-10-2018	5.8	Vu App of (su ver 12. Eas allo net con	lnerability plications Fr Oracle bcomponent sions that a 2.3, 12.2.4, sily exploi	E-Busines E: None). Ere affected a Electric 12.2.5 ar Electrication are services. Electric itable vues articated attaction are services.	http://ww e.com/teo k/securit advisory/ 018-4428	chnetwor y-	A-Ora- Appli/01- 11-18/13	
CV Scoring Scale (C	vss)	3-4	ŀ	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	ID	Reference	e/Patch	NCIIPC ID
	<b>Janagor</b>		per wh App ma provul una or App dat ins occasion (CV)	essible data (Confident pacts). 7SS:3.0/AV:N C:H/I:L/A:N)	han the atterability is Framework cly impact essful attactors to cracess to cramework unauthorize access to cations Factors Factors and CVSS (AC:L/PR:N	in Oracle , attacks additional ks of this esult in itical data all Oracle accessible ed update, o some of ramework Base Score Integrity Vector: N/UI:R/S:			
Applications M Gain	16-10-2018	5	17	lnerability	in the	Oracle	http://ww	urur omo al	A-Ora-
Information	10 10 2010		Apportant Apport	plications Macle E-bcomponent oported vers 12.1.3, 12 2.6 and 12.2 nerability al acker with TP to oplications acks of the ult in unauth subset of nager acces se Score bacts). VSS:3.0/AV:N C:L/I:N/A:N)	anager come. Business is Supportions that an 2.2.3, 12.2. 2.7. Easily end to the compromise Manager. It is vulneral and the compromise or acle Apportage App	re affected 4, 12.2.5, exploitable henticated access via e Oracle Successful bility can d access to oplications CVSS 3.0 ridentiality Vector: N/UI:N/S:	e.com/ted k/securit advisory/ 018-4428	chnetwor y- 'cpuoct2 3296.html	Appli/01- 11-18/14
NA	16-10-2018	5.8		lnerability plications M acle E	in the anager com Business		http://ww e.com/teo k/securit	chnetwor	A-Ora- Appli/01- 11-18/15
CV Scoring Scale (C	VSS)	3-4	ļ.	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	ID	Reference	e/Patch	NCIIPC ID
Business Intel	igança		vers 12.2 vuli atta HTT App atta is i atta add atta resu crit Ora acco una acco una acco una acco (CV	nerability alacker with TP to oblications a personance of the content of the cont	re affected at 12.2.5, 1 asily a lows unaut network a compromise Manager. It has been been been been been been been bee	are 12.1.3, 2.2.6 and exploitable henticated access via e Oracle Successful nteraction than the lnerability Manager, y impact Successful bility can access to all Manager well as tor delete oplications CVSS 3.0 tiality and S Vector: N/UI:R/S:		cpuoct2 3296.html	
	. —	r o	171	ان معمل الناد ان	m the Oweel	Dugingg	lattra / /r.rr	uru ono ol	A O==
NA	16-10-2018	5.8	Intecom Mid Ana vers Eas allo net com Inte Suc inte	nponent of deleware sion that is ily exploit was unauthe work acceptomise elligence cessful attaction from	Enterprise of Oracle (subcover). The affected is itable vu nticated attaces via Oracle Enterprise acks requinent a person with	Edition Fusion omponent: supported 12.2.1.3.0. lnerability acker with HTTP to Business Edition. re human other than hile the	e.com/teo k/securit advisory/	chnetwor y-	A-Ora- Busin/01- 11-18/16
CV Scoring Scale (C	VSS)	3-4	ļ	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Descri	ption&CVE_	ID	Reference	e/Patch	NCIIPC ID
Type(s)			attacks may additional p attacks of th result in una critical data or	oroducts. his vulneral nuthorized complete action accessift horized upd ss to some elligence sible data. 2 (Confident acts). CVS	Successful bility can access to all access to all atelligence ole data as ate, insert of Oracle Enterprise CVSS 3.0 tiality and S Vector: N/UI:R/S:			
Connector/j								
NA	16-10-2018	6.5	allows low pri	(subconsupported dare 8.0.12 ditable vulvileged attaces via compromist ccessful attaces	of Oracle omponent: versions and prior. Inerability acker with multiple te MySQL acks of this a takeover S 3.0 Base to Integrity ts). CVSS	https://s etapp.cor ry/ntap- 2018101	n/adviso	A-Ora- Conne/01- 11-18/17
Customer Inter								
NA	16-10-2018	5.8	Vulnerability i Interaction Hi Oracle E (subcomponen Supported vers are 12.1.1, 12.	k/securit advisory,	chnetwor y-	A-Ora- Custo/01- 11-18/18		
CV Scoring Scale (CV	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type( Injection; XSS- Cros		Request F	Forgery; Dir. TravDi	irectory Traver	sal; DoS-Denia	al of Service;	NA- Not Appli	cable; Sql-SQL

CV Scoring Scal	o (CVSS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10
NA NA	16-10-2018	7.5	com Servaffe 12.2 vultatta mul Java vulta of J (Co Ava (CV	nerability aponent of ver. Suppor cted are 2.0.1 and 1 nerability al cker with tiple proto a VM. Succe nerability of ava VM. CV anfidentiality ilability im SS:3.0/AV:N a:H/I:H/A:H	of Oracle red version 11.2.0.4, 8c. Easily lows unaut network ocols to coessful attacan result in SS 3.0 Bases, Integrapacts). CV	12.1.0.2, exploitable chenticated access via empromise cks of this a takeover e Score 9.8 eity and SS Vector: N/UI:N/S:	e.com/te k/securi advisory 018-442	ww.oracl echnetwor ty- cpuoct2 8296.html	A-Ora- Datab/01- 11-18/19
Database So	orver		Histimp Suc vuliuna or Cus accouna account (CVS) (Coimp (CVS)	cessful nerability uthorized a complete tomer I essible d uthorized u ess to some raction His S 3.0 nfidentiality acts). SS:3.0/AV:N :H/I:L/A:N)	ks may siditional attacks can reaccess to enaccess to enaccess to enacces to enacces as pdate, inserted of Oracle story access Base Soy and CVSS	ignificantly products. of this esult in citical data all Oracle History well as ct or delete Customer sible data. core 8.2 Integrity Vector: N/UI:R/S:			
			com Inte atta from atta	cks requir n a pers cker and w	Oracle History. e human on other while the vu	than the Ilnerability			

Description&CVE\_ID

vulnerability

allows

Reference/Patch

NCIIPC ID

Vulnerability Type(s)

**Publish Date** 

CVSS

exploitable

Vulnerability	<b>Publish Date</b>	CVSS		Descrip	tion&CVE_	_ID	Referen	ce/Patch	NCIIPC ID
Type(s)  Demantra Dem	l nand Managem	ent							
NA	16-10-2018	4.3	Der Orac (sur Supare vull atta HTT Der Suc into the this una accordant (In (CV U/O	mantra De cessful atta eraction from a attacker. So wilnerabit each orized understand Manta. CVSS 3 tegrity imp/SS:3.0/AV:NC:N/I:L/A:N)	gement come Chain Product ions that a general mand mand mand mand mand its required a person of Oracle agement of Base acts). CVS /AC:L/PR:1	apponent of lucts Suite Security). The affected exploitable henticated access via the Oracle magement. The human other than attacks of result in the Demantra accessible Score 4.3 S Vector: N/UI:R/S:	e.com/te k/securit advisory	ww.oracl chnetwor ty- /cpuoct2 8296.html	A-0ra- Deman/01 -11-18/20
E-business Inte	elliaence		31	Z <sup>*</sup> /					
NA NA	16-10-2018	5.8	Bus Orac (su Page ver 12. vul atta HT Bus atta fro atta add atta add atta	siness Intellicate Educomponent ge/Report Resions that an 12.1 and 12.1 acker with TP to consiness Interacks required acker and win Oracle Educks may	gence come Business endering). re affected 1.3. Easily enderwork and network and promise elligence. en human in on other hile the vurant business Ir significant roducts.	Suite Overview Supported are 12.1.1, exploitable henticated access via Oracle E- Successful interaction than the linerability itelligence, y impact Successful bility can	e.com/te k/securit advisory	ww.oracl chnetwor ty- /cpuoct2 8296.html	A-Ora-E- bus/01- 11-18/21
CV Scoring Scale (C	VSS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10
	(s): CSRF-Cross Site	Request F	orgei	ry; Dir. TravDi	rectory Travei	rsal; DoS-Denia	al of Service;	NA- Not Appli	cable; Sql-SQI

Vulnerability Publish Date	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)		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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Email/01- 11-18/22
Endeca Information Discove				
NA 16-10-2018	5.8	Vulnerability in the Oracle Endeca Information Discovery Integrator component of Oracle Fusion Middleware (subcomponent:	http://www.oracl e.com/technetwor k/security- advisory/cpuoct2	A-Ora- Endec/01- 11-18/23
CV Scoring Scale (CVSS)	3-4	4 4-5 5-6 6-7  Forgery; Dir. TravDirectory Traversal; DoS-Denia	7-8 8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	ID	Reference	e/Patch	NCIIPC ID
Type(s)			thar East allo net con Info Such interest the this una account of Dis CVS (Co imp (CV)	ows unautherwork accempromise ormation Excessful attacker. So will authorized underston I covery Integracts).  SS 3.0 onfidentiality pacts).  SC:L/I:L/A:N)	d are 3.1.0 itable vulnticated attacts via loss via los via loss via loss via loss v	and 3.2.0. Inerability acker with HTTP to Endeca Integrator. The human other than attacks of result in tor delete Endeca Integrator well as to a subset of a subset of the firmation sible data. The subset of the s	018-4428	3296.html	
DoS	16-10-2018	6.8	Ser Mid Ser that exp una net con Suc inte this una modall (dat	nerability inver componduleware (inver Faces). It is affect to a secondary in the face of	tent of Orac subcomponers of the support of the support of the support of the support of the subcomponers of the support of th	cle Fusion ent: Java ed version .2. Easily allows er with HTTP to ish Server. The human other than attacks of result in eletion or cal data or accessible zed access	e.com/ted k/securit advisory/ 018-4428	chnetwor y- 'cpuoct2	A-Ora- Glass/01- 11-18/24
CV Scoring Scale (C	VSS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(з)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Glass/01- 11-18/26

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

Vulnerability Type(s)	<b>Publish Date</b>	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	I				1
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.tena ble.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.tena ble.com/security/ research/tra- 2018-31	A-0ra- Golde/01- 11-18/28
		3-4	4-5 5-6 6-7	7-8 8-9	9-10

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID				Referen	ce/Patch	NCIIPC ID
Турс(з)			29:	14					
Overflow	16-10-2018	7.5	Vulue Gold Mover 12. East allow with Gold important of Line CVS (Condition of CVS) (Condi	nerability denGate nitoring M sions that 1.2.1.0, 12.2 sily exploit ows unauther work acces npromise hile the vuln denGate, attract accessful a nerability ca Oracle Gol ux and Wir SS score i nplexity as tforms, the SS 3.0 onfidentiality ailability im VSS:3.0/AV:N C:H/I:H/A:H)	(subcoanager).  are afferonce of the control of the		vww.tena security/ /tra-	A-Ora- Golde/01- 11-18/29	
	iise Fleet Manag			1 -1	1	0 1	1	<u> </u>	4.0
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			e.com/te k/securit advisory 018-442	/cpuoct2 8296.html	A-Ora- Hospi/01- 11-18/30	
CV Scoring Scale (C	<u>-</u>	3-4		4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type Injection; XSS- Cros	(s): CSRF-Cross Site s Site Scripting;	Request F	orger	ry; Dir. TravDi	ectory Traver	rsal; DoS-Denia	al of Service;	NA- Not Appli	cable; Sql-SQL

Vulnerability Type(s)	<b>Publish Date</b>	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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Hospi/01- 11-18/32

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

Typo(c)		CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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	k/security-advisory/cpuoct2 018-4428296.html	A-0ra- Hospi/01- 11-18/33
			Management System	1,	
NA	16-10-2018	4.4	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System	e.com/technetwor	A-Ora- Hospi/01- 11-18/34
CV Scoring Scale (CV	'SS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10

		to compromise O Gift and Loyalty. Suc this vulnerability	ccessful attack	s of		
Hospitality Gift And NA 16	-10-2018	supported version of the second supported version of the second support of the second su	and Loy racle Food ications. that is affected by all attacker have been been been been been been been be	alty e.c. and k/s The adv d is 01s ility ving the acle utes	om/tech security visory/c	A-Ora- Hospi/01 11-18/35
		Management Syste significantly imp products. Successfu vulnerability can re	em, attacks repact additional attacks of esult in takeo spitality Crusty Managem Base Score Integrity es). CVSS Veces.L/PR:H/UI:R/	may onal this over uise nent 7.7 and etor:		
		Hospitality Crui Property Manago Successful attacks Interaction from a p	able vulnerabinged attacker versite who cruise Shipbon promise Oracise Shipbon Systement While Oracle Hospita	ility with here bard tem acle bard tem. man than the ality		

Description&CVE\_ID

component of Oracle Hospitality

NCIIPC ID

Reference/Patch

advisory/cpuoct2

Vulnerability

Type(s)

**Publish Date** 

CVSS

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
			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		
	porting And An				
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Hospi/01- 11-18/36
Hyperion					

	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CVSS)	0.1	1.5	3 0	0 /	, 0		7 10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
NA 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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	5, 1	A-0ra- Hyper/01- 11-18/44

	2.4	4.5	F C	( F	7.0	0.0	0.40
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	/-8	8-9	9-10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)	16-10-2018	5.8	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  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:	http://www.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Hyper/01- 11-18/45
			(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S: C/C:L/I:L/A:N). <b>CVE-ID:CVE-2018-</b> <b>3140</b>		
Hyperion Com	ı		**	-	
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	k/security- advisory/cpuoct2	A-Ora- Hyper/01- 11-18/38
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
		Request F	orgery; Dir. TravDirectory Traversal; DoS-Deni	al of Service; NA- Not Appli	cable; Sql-SQL

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
NA	16-10-2018	5.8	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  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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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)	<b>Publish Date</b>	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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Hyper/01- 11-18/41

ava i a i cavaa	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CVSS)							

Vulnerability	<b>Publish Date</b>	CVSS		Descrip	tion&CVE_	Reference	e/Patch	NCIIPC ID	
Type(s)			Ever hur oth vul Ever imp Suc vul una acc Ever una of acc 6.1 imp (CV	ents. Succes man interace than the anerability is ents, attack eact additional anerability nuthorized upers to some ents accessible data. (Confident eacts).  SS:3.0/AV:NC:L/I:L/A:N).	tion from attacker and in Hyperior s may sig litional attacks can re pdate, inser of Hyperior ble data ac ead access t Common CVSS 3.0 E ciality and CVSS	a person I while the n Common gnificantly products. of this sult in t or delete n Common s well as no a subset Events Base Score Integrity Vector: N/UI:R/S:			
Hyperion Data	Relationship M	lanaaen							
NA	16-10-2018	4	Vull Rel con (su Sec is exp privacc Hyp Mais sign pro vull una acc 7.7	nerability in ationship of the property of the same of	Ma f Oracle : Acces upported ve 11.1.2.4.34 nerability a ncker with TTP to co Data Re While the vu n Data Re attacks impact essful attac can re ccess to cr ccess to all nship Ma	e.com/ted k/securit advisory/	chnetwor y-	A-0ra- Hyper/01- 11-18/42	
CV Scoring Scale (C	VSS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	_ID	Referen	ce/Patch	NCIIPC ID
, pe (3)				/SS:3.0/AV:N H/I:N/A:N). <b>08</b>					
<b>Identity Analyt</b>	tics								
NA	16-10-2018	5.5	Ana Fus Cor ver Eas allo net com Ana vul una mo all acc una of acc 7.1 imp (CV	sion Middley re Compone sion that is sily exploi ows low pri work acce npromise alytics. Succ nerability authorized of dification ac Oracle essible da authorized re Confident oacts). CSS:3.0/AV:N	nponent ovare (subconts). The affected is affected is attacked attacked attacked attacked attacked attacked access to critical as a access to a access to a access to a access to access t	of Oracle omponent: supported 11.1.1.5.8. Inerability acker with HTTP to Identity cks of this esult in eletion or cal data or Analytics well as to a subset Analytics Base Score Integrity Vector: L/UI:N/S:	e.com/te k/securit advisory	ww.oracl chnetwor ty- /cpuoct2 8296.html	A-0ra- Ident/01- 11-18/46
Identity Manag	ger								
DoS	16-10-2018	6.4	Mai Mic Adv ver 11. exp una net con Mai in mai pro vul	sions that 1.2.3.0 and coloitable venthenticated work acces inpromise inager. While Oracle Identy oracles Succes inpromises inguities in	onent of Ora (subconsole). are affel 1 12.2.1.3. Tulnerability d attack ess via Oracle to the vulne tity Manage cly impact essful attack can re	acle Fusion omponent: Supported ected are 0. Easily allows er with HTTP to Identity erability is er, attacks additional eks of this esult in	e.com/te k/securit advisory 018-442	chnetwor ty- /cpuoct2 8296.html	A-0ra- Ident/01- 11-18/47
CV Scoring Scale (C	VSS)	3-4	ŀ	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type Injection; XSS- Cros	(s): CSRF-Cross Site ss Site Scripting;	Request I	orger	y; Dir. TravDi	rectory Traver	rsal; DoS-Denia	al of Service;	NA- Not Appli	cable; Sql-SQL

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	tion&CVE_	ID	Reference	ce/Patch	NCIIPC ID	
Турс(з)			of (dat cau (pa Mar (Co imp (CV)	authorized re Oracle Identica and una use a partia artial DOS) nager. CVSS onfidentiality pacts). /SS:3.0/AV:N C:L/I:N/A:L).	ty Manager uthorized al denial of of Oracle 3.0 Base and A CVSS /AC:L/PR:N					
Ilearning			1				1			
NA	16-10-2018	5.8	con (su Adu tha Eas allo net con Suc inte vul atta ado atta res crit Ora wel or iLe Bas Inte (CV	nerability is acks may ditional pracks of this cult in unactical data or eacle iLearning las unauth delete accessore 8.2 egrity imparts:3.0/AV:NC:H/I:L/A:N)	Confidents  Confidents	iLearning Learner d versions and 6.2. lnerability acker with HTTP to iLearning re human other than hile the iLearning, y impact Successful bility can access to ccess to all le data as ate, insert of Oracle CVSS 3.0 tiality and S Vector: N/UI:R/S:	e.com/te/ k/securit advisory/	chnetwor y-	A-Ora- Ilear/01- 11-18/48	
<i>Iprocurement</i>			1				1 -			
NA	16-10-2018	5	Vulnerability in the Oracle http://www.oracl iProcurement component of Oracle e.com/technetwor Iproc/01-E-Business Suite (subcomponent: E- k/security- 11-18/49							
CV Scoring Scale (C	CV Scoring Scale (CVSS) 3-4 4-5 5-6 6-7 7-8 8-9 9-10									
Vulnerability Type Injection; XSS- Cros	(s): CSRF-Cross Site s Site Scripting;	Request F	orger	ry; Dir. TravDii	ectory Traver	sal; DoS-Denia	al of Service; l	NA- Not Appli	cable; Sql-SQL	

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Descr	iption&CVE_	ID	Reference	e/Patch	NCIIPC ID
Type(s)			Supported ver are 12.1.1, 1 12.2.4, 12.2.5	12.1.2, 12.1. 5, 12.2.6 are oitable vuluenticated attacks or can reaccess to craccess to c	advisory/ 018-4428	cpuoct2 3296.html		
NA NA	16-10-2018	5.8	interface). Su are affected ar 12.2.3, 12.2.4	of Oracle In becomponent: pported verse 12.1.1, 12.2.5, 12.2.5, 12.2.5, 13.2.5, 14.2.2.5, 15.2.5, 15.2.5, 15.2.5, 16.2	http://ww e.com/teo k/securit advisory/ 018-4428	chnetwor y-	A-0ra- Istor/01- 11-18/50	
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)

Vulnerability	<b>Publish Date</b>	CVSS		Descri	ption&CVE	E_ID	Reference	ce/Patch	NCIIPC ID
Type(s)			(CV			Vector: :N/UI:R/S: :CVE-2018-			
JDK,JRE									
Execute Code	16-10-2018	3.3	Em SE Supare Em vul attainfi Em Jav Sucinte this una or of SE This dep run apprace apprace the vul dep that (e.g adr can	bedded cor (subcomported ver ported ver ported ver ported ser ported ser ported externation from attacker. It is a vulnerable and ser ported externation from a tracker. It is a vulnerable ser ported externation from the ported externation of the ported	nponent of onent: Services that a secures to critically accessible of typically poxed Java or sandboard SE 8), the code (e.g., e internet) box for secure application only transtalled. This we exploited of functionals	SE, Java SE ompromise Embedded. ire human other than attacks of result in deletion or cical data or Embedded well as critical data ava SE, Java data. Note: es to Java in clients Web Start	om/advis -2018101 0001/,htt	errata/R 02,https:/ .netapp.c sory/ntap 18- tps://acc st.com/er	A-0ra- JDK,J/01- 11-18/51
		3-4	<u>.</u>	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)

Vulnerability Type(s)	<b>Publish Date</b>	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.n etapp.com/adviso ry/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.n etapp.com/adviso ry/ntap- 20181018- 0001/,https://usn .ubuntu.com/3804 -1/	A-Ora- JDK,J/01- 11-18/53

	2.4	4.5	F C	( F	7.0	0.0	0.40
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	/-8	8-9	9-10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)	16-10-2018	5.1	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  Vulnerability in the Java SE	https://security.n	A-Ora-
IVA	10-10-2018	5.1	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	etapp.com/adviso ry/ntap- 20181018- 0001/,https://acc ess.redhat.com/er rata/RHSA- 2018:3003,https:/ /access.redhat.co m/errata/RHSA- 2018:3002	A-0ra- 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)	<b>Publish Date</b>	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
Micros Retail-j			
NA	16-10-2018	5	Vulnerability in the MICROS Retail-J component of Oracle Retail e.com/technetwor Applications (subcomponent: k/security-advisory/cpuoct2 version that is affected is 12.1.2. Easily exploitable vulnerability http://www.oracl e.com/technetwor k/security-advisory/cpuoct2 018-4428296.html
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7 7-8 8-9 9-10
		Request F	orgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

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. Successful with metwork access via HTTP to 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 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)/AN:M/ACL/PR:N/UI:N/S: U/C:L/I:L/A:N). CVE-ID:CVE-2018-  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 albuntu.com/3799 1.1  CV Scoring Scale (CVSS) 4-5 6-6 6-7 7-8 8-9 9-10	Vulnerability	<b>Publish Date</b>	CVSS	Descrip	otion&CVE_	ID	Reference	ce/Patch	NCIIPC ID
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-I. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MICROS Retail-I accessible data as well as unauthorized read access to a subset of MICROS Retail-I 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  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 .ubuntu.com/3799 and prior and 8.0.12 and prior. Difficult to exploit vulnerability .ubuntu.com/3799 inlows high privileged attacker with 1.1	Type(s)			network acce compromise Successful vulnerability unauthorized a or complete a Retail-J access Base Score impacts). (CVSS:3.0/AV:N U/C:H/I:N/A:N	ess via l MICROS attacks can reaccess to cr ccess to al ible data. 7.5 (Conf CVSS	HTTP to Retail-J. of this sult in itical data l MICROS CVSS 3.0 identiality Vector: I/UI:N/S:			
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  3.4  3.5  Vulnerability in the MySQL Server com/adviso Mysql/01-11-18/58  A-Ora-MysQL ory/ntap- 20181018- 0002/,https://usn .ubuntu.com/3799 -1/		16-10-2018	6.4	Vulnerability in component Applications (Office). Support affected are 13 exploitable with unauthenticated network accessful accessful vulnerability unauthorized with access to some accessible day unauthorized roof MICROS Recurrent CVSS 3.0 (Confidentiality impacts). (CVSS:3.0/AV:NU/C:L/I:L/A:N)	of Oracle subcompone ted version .0.0 and 12. vulnerability d attacked ses via I MICROS attacks can repdate, insere of MICRO ata as ead access the tail-J access the control of the contro	Retail ent: Back s that are 1.2. Easily allows er with HTTP to Retail-J. of this sult in tor delete S Retail-J well as o a subset sible data. ore 6.5 Integrity Vector: I/UI:N/S:	e.com/te/k/securit	chnetwor y- /cpuoct2	Micro/01-
component of Oracle MySQL etapp.com/adviso (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 of the supplementary of the supplementary and substituting and prior and 8.0.12 are supplementary and prior of the supplementary of the supplementa		16-10-2018	3.5	Vulnerability i	n the MvS(	OL Server	https://s	ecurity.n	A-Ora-
CV Scoring Scale (CVSS) 3-4 4-5 5-6 6-7 7-8 8-9 9-10				component of (subcomponent versions that a and prior and Difficult to	etapp.cor ry/ntap- 2018101 0002/,ht .ubuntu.c	n/adviso 8- tps://usn	Mysql/01-		
	CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.n etapp.com/adviso ry/ntap- 20181018- 0002/,https://usn .ubuntu.com/3799 -1/	A-0ra- 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.n etapp.com/adviso ry/ntap- 20181018- 0002/,https://usn .ubuntu.com/3799 -1/	A-Ora- Mysql/01- 11-18/60

	2.4	4.5	F C	( F	7.0	0.0	0.40
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	/-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	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.n etapp.com/adviso ry/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.ubunt u.com/3799- 1/,https://securit y.netapp.com/advi sory/ntap- 20181018-0002/	A-0ra- Mysql/01- 11-18/62

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Descri	ption&CVE_	ID	Reference	ce/Patch	NCIIPC ID
Туре(з)			U/C:N/I:N/A:H <b>3251</b>	). CVE-ID:(	CVE-2018-			
NA	16-10-2018	4	(subcomponent versions that a and prior and 8 exploitable vul privileged att access via more compromise Successful vulnerability unauthorized a or frequently (complete DO CVSS 3.0 Base impacts).  (CVSS:3.0/AV:10/C:N/I:N/A:H 3162	of Oracle t: InnoDB). are affected 3.0.12 and properties of the pr	MySQL Supported are 5.7.23 rior. Easily llows high network otocols to Server. of this esult in use a hang ole crash QL Server. availability Vector: H/UI:N/S:	.ubuntu.c	n/adviso 8- tps://usn om/3799	A-0ra- Mysql/01- 11-18/63
NA	16-10-2018	4	(subcomponent versions that a and prior and 8 exploitable vul privileged attaccess via maccess via maccessful vulnerability unauthorized a	of Oracle t: InnoDB). are affected 3.0.12 and properties of the pr	MySQL Supported are 5.7.23 rior. Easily llows high network btocols to Server. of this esult in use a hang ble crash QL Server. Availability Vector: H/UI:N/S:		n/adviso	A-0ra- Mysql/01- 11-18/64
NA	16-10-2018	4	Vulnerability i	of Oracle	MySQL	https://setapp.com	•	A-Ora- Mysql/01- 11-18/65
CV Scoring Scale (C	VSS)	3-4	•	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.n etapp.com/adviso ry/ntap- 20181018- 0002/,https://usn .ubuntu.com/3799 -1/	A-0ra- 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.n etapp.com/adviso ry/ntap- 20181018-0002/	A-0ra- Mysql/01- 11-18/67

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

Vulnerability Publish Date Type(s)		CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.n etapp.com/adviso ry/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.n etapp.com/adviso ry/ntap- 20181018-0002/	A-0ra- Mysql/01- 11-18/69

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(з)			(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.ubunt u.com/3799- 1/,https://securit y.netapp.com/advi sory/ntap- 20181018-0002/	A-0ra- 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.n etapp.com/adviso ry/ntap- 20181018-0002/	A-0ra- Mysql/01- 11-18/71

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			U/C:N/I:N/A:H). <b>CVE-ID:CVE-2018- 3186</b>		
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.n etapp.com/adviso ry/ntap- 20181018-0002/	A-0ra- 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.n etapp.com/adviso ry/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.ubunt u.com/3799- 2/,https://usn.ub	A-Ora- Mysql/01- 11-18/74

	2.4	4.5	F C	( F	7.0	0.0	0.40
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	/-8	8-9	9-10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
NA NA	16-10-2018	4	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  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	untu.com/3799- 1/,https://securit y.netapp.com/advi sory/ntap- 20181018-0002/  https://usn.ubunt u.com/3799- 1/,https://securit y.netapp.com/advi sory/ntap- 20181018-0002/	A-0ra- Mysql/01- 11-18/75
NA	16-10-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser).	https://security.n etapp.com/adviso ry/ntap-	A-Ora- Mysql/01- 11-18/76
			Supported versions that are affected	20181018-0002/	

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

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.ubunt u.com/3799- 1/,https://securit y.netapp.com/advi sory/ntap- 20181018-0002/	A-0ra- 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.ubunt u.com/3799- 1/,https://securit y.netapp.com/advi sory/ntap- 20181018-0002/	A-0ra- Mysql/01- 11-18/78

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.n etapp.com/adviso ry/ntap- 20181018-0002/	A-0ra- 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.n etapp.com/adviso ry/ntap- 20181018-0002/	A-0ra- Mysql/01- 11-18/80

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Туре(з)			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-	etapp.com/adviso ry/ntap- 20181018- 0002/,https://usn .ubuntu.com/3799	A-0ra- Mysql/01- 11-18/82

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
0 ( )							

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			2144		
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.n etapp.com/adviso ry/ntap- 20181018- 0002/,https://usn .ubuntu.com/3799 -1/	A-0ra- 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.n etapp.com/adviso ry/ntap- 20181018- 0002/,https://usn .ubuntu.com/3799 -1/	A-0ra- Mysql/01- 11-18/84

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(з)			U/C:N/I:L/A:H). <b>CVE-ID:CVE-2018- 3185</b>		
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.n etapp.com/adviso ry/ntap- 20181018-0002/	A-0ra- 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.n etapp.com/adviso ry/ntap- 20181018- 0002/,https://usn .ubuntu.com/3799 -1/	A-0ra- Mysql/01- 11-18/86

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
0 ( )							

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID			ID	Reference	e/Patch	NCIIPC ID
Туре(s)			(CV U/0	oacts). /SS:3.0/AV:N C:N/I:L/A:H) <b>47</b>	, ,	, ,			
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://se etapp.com ry/ntap- 20181013 0002/,htt .ubuntu.c -1/	n/adviso 8-	A-0ra- Mysql/01- 11-18/87
Outside In Tech			ı				T		
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			e.com/teo k/securit advisory/	chnetwor y-	A-Ora- Outsi/01- 11-18/88	
CV Scoring Scale (C	VSS)	3-4	ļ	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
DoS	16-10-2018	5.8	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  Vulnerability in the Oracle Outside In	http://www.oracl	A-Ora-
D03	10-10-2016	3.0	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	e.com/technetwork/security-advisory/cpuoct2018-4428296.html	Outsi/01- 11-18/89

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
NA NA	16-10-2018	4.3	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  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 directly to Outside In Technology code, but if data is not received over a network directly to Outside In Technology code, but if data is not received over a network directly to Outside In Technology code, but if data is not received over a network directly to Outside In Technology code, but if data is not 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
			impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S: U/C:L/I:N/A:N). <b>CVE-ID:CVE-2018-3147</b>		
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 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- Outsi/01- 11-18/91
NA	16-10-2018	5.8	Vulnerability in the Oracle Outside In	http://www.oracl	A-Ora-
			Technology component of Oracle Fusion Middleware (subcomponent:	e.com/technetwor k/security-	Outsi/01- 11-18/92
			rusion middleware (subcomponent:	K/security-	11-18/92

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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 accessible data. Note: Outside In Technology accessible data. Note: 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/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 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)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
NA	16-10-2018	5.8	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 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  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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)	16 10 2010	ro	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		A Ovo
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Outsi/01- 11-18/95

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- Outsi/01- 11-18/96

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Vulnerability Type(s)  NA	16-10-2018	5.8	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  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- 11-18/97
NA	16-10-2018	5.8	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.oracl	A-Ora-
INA	10-10-2018	3.8	Technology component of Oracle	e.com/technetwor	A-Ora- Outsi/01-

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

Vulnerability Type(s)	<b>Publish Date</b>	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 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 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/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- Outsi/01- 11-18/99
			45 56 67	7.0	

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Outsi/01- 11-18/100

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			(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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- Outsi/01- 11-18/101

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)	16.10.2010		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 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Outsi/01- 11-18/102

	2.4	4.5	F C	( F	7.0	0.0	0.40
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	/-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	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 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
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 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 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-	http://www.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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
** 1 1 1 1 1 C C C C C C C C C C C C C C				1 - 2 - 1			11 6 1667

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 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)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
NA	16-10-2018	5.8	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  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 critical data or complete access to some of 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 0utsi/01- 11-18/107

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

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/U: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 Partner Management component of Oracle Partner 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. Successful attacks require human interaction from a person other than the attacker and while the vulnerability in result in unauthorized access to critical data or complete access to critical data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data as well as unauthorized update, insert or delete access to some of 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:	Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	ID	Reference	e/Patch	NCIIPC ID
NA  16-10-2018    S.8				dev pro the Tec ass dat to 0 dat the 3.0 and (CV U/0	velopment of tocol and Control	kits (SDI VSS score of at uses the de. The C' the softwa ver a netwo echnology of eived over a may be lo e 7.1 (Confi mpacts). CV	Ks). The depend on Outside In VSS score re passes rk directly code, but if a network wer. CVSS dentiality SS Vector: N/UI:R/S:			
Management component of Oracle E-Business Suite (subcomponent: k/security-advisory/cpuoct2 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:			E O	171	novohility i	a tha Oracl	la Dantnan	http://run	umur oma al	A One
CV Scoring Scale (CVSS) 3-4 4-5 5-6 6-7 7-8 8-9 9-10	IVA	10-10-2018	3.0	Mai Bus Par ver 12. 12. vul atta HT Mai req per wh Par sign pro vul una or Par as inso Ora acc 8.2	nagement cosiness Suitner Dash sions that at 1.2, 12.1.3, 2.6 and 12.2 nerability alacker with TP to compragement. The compragement of the vulnation of the the vuln	omponent of te (subcomboard). The affected of 12.2.3, 12.2 2.7. Easily ellows unauthous of the attention of	f Oracle E- component: Supported are 12.1.1, 2.4, 12.2.5, exploitable henticated access via ele Partner attacks in from a acker and in Oracle acks may additional els of this esult in etical data all Oracle ssible data d update, o some of anagement Base Score Integrity	e.com/teck/securit advisory/ 018-4428	chnetwor y- /cpuoct2	Partn/01-
	CV Scoring Scale (C	VSS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	tion&CVE_	.ID	Referen	ce/Patch	NCIIPC ID
Турс(з)				/SS:3.0/AV:N C:H/I:L/A:N) <b>96</b>					
Peoplesoft Ente	erprise Interact	tion Hul	)						
NA	16-10-2018	5.5					e.com/te k/securit advisory	chnetwor	A-Ora- Peopl/01- 11-18/109
<b>Peoplesoft Ent</b>	erprise People	tools							
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				k/securit advisory 018-442	chnetwor	A-0ra- Peopl/01- 11-18/110
CV Scoring Scale (C	VSS)	3-4	ŀ	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type Injection; XSS- Cros	(s): CSRF-Cross Site ss Site Scripting;	Request I	orgei	ry; Dir. TravDi	rectory Travei	rsal; DoS-Denia	al of Service;	NA- Not Appli	cable; Sql-SQL

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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:	e.com/technetwor k/security- advisory/cpuoct2	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)	<b>Publish Date</b>	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). <b>CVE-ID:CVE-2018-</b> <b>3261</b>		
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Peopl/01- 11-18/115

	0.4	4 -	F (	( <b>=</b>	7.0	0.0	0.40
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)	46.40.0016	_	Y 1 100 1 2 2 2	1	A C
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Peopl/01- 11-18/117

	2.4	4.5	F C	( F	7.0	0.0	0.40
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	/-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(з)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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
0 ( )							

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)  NA	16-10-2018	5.8	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  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	http://www.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Peopl/01- 11-18/120
	1		or delete access to some of		

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

Vulnerability			Reference/Patch	NCIIPC ID	
Type(s)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security-	A-Ora- Peopl/01- 11-18/122

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
			(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/cpuoct2 018-4428296.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	e.com/technetwor	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			Reference/Patch	NCIIPC ID	
Type(s)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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
-------------------------	-----	-----	-----	-----	-----	-----	------

i .		0454		
		3154		
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Peopl/01- 11-18/125
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Peopl/01- 11-18/126
			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  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	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  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

CV Scoring Scale (CVSS)							
Vulnerability Type(s): CSRF-Cross Site	Request Forger	y; Dir. TravDirec	tory Traver	sal; DoS-Deni	ial of Service; l	NA- Not Applica	able; Sql-SQL

Vulnerability Publish Date Type(s)		CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(з)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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)			Description&CVE_ID	Reference/Patch	NCIIPC ID
Туре(з)			(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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Peopl/01- 11-18/129

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	ID	Reference	e/Patch	NCIIPC ID				
	16 10 2010		Ento atta resu Ento Bas Inte CVS (CV U/O 319	erprise Peocks of the old in take erprise Peoce Score egrity and SS:3.0/AV:N:H/I:H/A:H	npromise opleTools. is vulneral eover of opleTools. 7.2 (Confidential Availability I/AC:L/PR:H). CVE-ID:C		,						
NA	16-10-2018	6.5	Ente of (sub vers and vult atta HTT Ente atta resu Ente Bas Inte CVS (CV	Oracle Focomponents on that a 8.56. herability a cker with TP to concerprise Pecks of that in take erprise Pecks of the Score error and S SS:3.0/AV:N:H/I:H/A:H	in the in pleTools of PeopleSoft to SQR). The areaffected Easily to Easily t	http://ww e.com/teo k/security advisory/ 018-4428	chnetwor y- 'cpuoct2	A-Ora- Peopl/01- 11-18/130					
Primavera P6	Enterprise Proj	ect Port	folio	Manageme	ent								
NA	16-10-2018	5.8	Ente Mar Con (sub Sup are 17.1 vulr atta HTT	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				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			http://wv e.com/teo k/securit; advisory/ 018-4428	chnetwor y- 'cpuoct2	A-Ora- Prima/01- 11-18/131
CV Scoring Scale (C	VSS)	3-4	1	4-5	5-6	6-7	7-8	8-9	9-10				

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
NA NA	16-10-2018	5.8	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  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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Prima/01- 11-18/132

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Primavera Uni	fior		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		
NA NA	16-10-2018	5.8	Vulnerability in the Primavera	http://www.oracl	A-Ora-
Retail Open Co.	mmerce Platfor	·m	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	e.com/technetwor k/security-advisory/cpuoct2 018-4428296.html	Prima/01- 11-18/133
pon do					

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. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL											
Injection; XSS- Cross Site Scripting;											

9-10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID			Reference	e/Patch	NCIIPC ID	
NA NA	16-10-2018	4.9	Ope con App Inte tha 5.3 allo net con Cor atta res del crit Cor as crit Ora Pla Bas Inte (CV U/O	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 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				ww.oracl chnetwor y- 'cpuoct2 3296.html	A-Ora- Retai/01- 11-18/134
DoS	16-10-2018	6	Sale Ope ver and vultatta HT' Sale in ( may pro vultuna or	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				ww.oracl chnetwor y- cpuoct2 3296.html	A-Ora- Retai/01- 11-18/135
CV Scoring Scale (C	vss)	3-4		4-5	5-6	6-7	7-8	8-9	9-10

Type(s)									
			or Ret una par of C Bas Inte CVS	/SS:3.0/AV:N ::H/I:L/A:L).	ss to some lit accessibl ability to service (pa Sales Audit 7.7 (Confi Availability	of Oracle e data and cause a artial DOS) t. CVSS 3.0 dentiality, impacts). Vector: L/UI:N/S:			
Retail Xstore Po	oint Of Service								
NA	16-10-2018	6	Xsto Ora (sul) Sup are to priv acco Ora Suc vull of Ser (Co Ava (CV	bcomponent oported vers 15.0.2, 16.0 exploit vuln vileged atta ess via H7 icle Retail Xs cessful a nerability ca Oracle Ret vice. CVSS nfidentiality illability im SS:3.0/AV:N	Service contail Aptions that and 17.0. erability all cker with TTP to contacts and result in ail Xstore 3.0 Base pacts). CVS /AC:H/PR:1	apponent of oplications fronment). The affected of the control of this at takeover point of the control of the	e.com/te k/securit advisory	•	A-0ra- Retai/01- 11-18/136
Siebel Ui Frame	work								
NA	16-10-2018	5.8	Framework component of Oracle e.com/technetwor Sieb					A-Ora- Siebe/01- 11-18/137	
CV Scoring Scale (CV	SS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	_ID	Reference	e/Patch	NCIIPC ID
			the vulner Frame impact Success Vulner unaut access Frame unaut of Sie data. (Confi impact (CVSS)	attacker rability ework, attention a	is in Sacks may siditional attacks can repetition of second secon	while the Siebel UI significantly products. of this esult in a control of this esult in a swell as to a subset accessible Score 6.1 Integrity Vector: N/UI:R/S:			
Text			0007						
NA	16-10-2018	5.8	composerved affected 12.2.0 vulner attack multiporacle requirements of the composer of the com	onent or. Supported are 10.1. Example protoce Text. The human other to the vuluation attacks of the control of the protoce of the control of	f Oracle ted version 1.2.0.4, 12 lasily cols unaut network a cols to c	exploitable chenticated access via ampromise l attacks on from a tacker and in Oracle ignificantly products. of this esult in use a hang ole crash the Text as late, insert of Oracle S 3.0 Base	http://wv e.com/teo k/security advisory/ 018-4428	chnetwor y- cpuoct2	A-Ora- Text/01- 11-18/138
CV Scoring Scale (C	VSS)	3-4		4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	tion&CVE_	.ID	Reference	e/Patch	NCIIPC ID
				'SS:3.0/AV:N C:N/I:L/A:H) <b>99</b>					
Trade Manage	ment								
NA	16-10-2018	5.8	Mai Bus Inte are 12 vul atta HT' Mai req per whi Tra sign pro vul una or Tra as inso Ora dat (Co imp (CV	nerability all acker with TP to comp nagement. uire human son other tile the vulnude Manage nificantly authorized a complete acted Manager well as uert or deleticle Trade Ma. CVSS 3 onfidentiality pacts). CSS:3.0/AV:NC:H/I:L/A:N)	omponent of (subcomported verice) 12.1.1, 12. 12.2.5, 1 Isily of lows unaut network aromise Oran Successful interaction intera	f Oracle E- nent: User sions that 1.2, 12.1.3, 2.2.6 and exploitable henticated access via acle Trade attacks on from a cacker and in Oracle acks may additional acks of this esult in ritical data all Oracle sible data d update, o some of accessible Score 8.2 Integrity Vector: N/UI:R/S:	http://ww e.com/teo k/securit advisory/ 018-4428	chnetwor y-	A-0ra- Trade/01- 11-18/139
User Managem			1				T		
NA	16-10-2018	5.5	Management component of Oracle E- Business Suite (subcomponent: k/se Reports). Supported versions that advi					ww.oracl chnetwor y- /cpuoct2 3296.html	A-Ora- User/01- 11-18/140
CV Scoring Scale (C	VSS)	3-4	ŀ	4-5	5-6	6-7	7-8	8-9	9-10
	(s): CSRF-Cross Site	Request F	orger	y; Dir. TravDi	rectory Traver	rsal; DoS-Denia	al of Service; I	NA- Not Appli	cable; Sql-SQL

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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		
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- Virtu/01- 11-18/141

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	/ <b>-</b> 8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site	<b>Request Forger</b>	y; Dir. TravDi	rectory Traver	sal; DoS-Deni	ial of Service; I	NA- Not Applic	able; Sql-SQL
Injection; XSS- Cross Site Scripting;							

5-6

6-7

7-8

8-9

9-10

4-5

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	ID	Reference	e/Patch	NCIIPC ID
Vm Virtualbox									
NA	16-10-2018	4.4	Virtal Vi	the infrastreated the infrastreated promise Outcessful attacker at	mponent of subcompond version to 5.2. Fulnerability d attacker where where we will be acks required and where we will be acks may significate the confident of	of Oracle ent: Core). that is 20. Easily allows with logon ere Oracle utes to virtualBox. The human other than while the racle VM gnificantly products. of this atakeover CVSS 3.0 identiality, impacts). Vector: I/UI:R/S:C	http://w e.com/tec k/securit advisory/ 018-4428	chnetwor y-	A-Ora- Vm/01- 11-18/142
NA	16-10-2018	4.4	Virt Virt The affe exp una to VM con Suc inte the vuli	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.				ww.oracl chnetwor y- /cpuoct2 3296.html	A-Ora- Vm/01- 11-18/143
CV Scoring Scale (C	VSS)	3-4	1	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(б)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(з)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Vm/01- 11-18/146

					= 0	0.0	0.10
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 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	e.com/technetwor k/security- advisory/cpuoct2	A-Ora- Vm/01- 11-18/148

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(b)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Vm/01- 11-18/150

	2.4	4.5	F C	( F	7.0	0.0	0.40
CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	/-8	8-9	9-10

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2	A-Ora- Vm/01- 11-18/152
	ı		**		

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
ev scoring scare (evss)							

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			affected is Prior to 5.2.20 Facily	018-4429206 html	
			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-	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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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)	<b>Publish Date</b>	CVSS		Descrip	otion&CVE_	.ID	Reference	e/Patch	NCIIPC ID
Type(s)				/SS:3.0/AV:L H/I:H/A:H). <b>98</b>					
NA	16-10-2018	6	Virt Virt The affe exp priv acc Ora atta fron atta is i may pro vuli of Bas Inte CVS (CV	'SS:3.0/AV:N H/I:H/A:H).	mponent of subcomponed version for to 5.2. Inerability and the RDP to continual Box. In the result of the subsection of the subsection of the subsection of the result in Virtual Box. In the subsection of the su	of Oracle ent: Core). that is 20. Easily allows low network empromise Successful nteraction than the lnerability ox, attacks additional eks of this a takeover CVSS 3.0 identiality, impacts). Vector: L/UI:R/S:C	http://ww e.com/teo k/securit advisory/ 018-4428	chnetwor y-	A-Ora- Vm/01- 11-18/154
Webcenter Por	1	_	l ,			Oracle			T
NA	16-10-2018	5	We Ora (su App that 12 wull atta HT" We of una of accc 5.3	nerability alacker with TP to o bCenter Por this vulner outhorized re Oracle essible data (Confident	sion M : WebCent Supported ed are 11.1 Easily e lows unaut network a compromise tal. Success ability can ead access t WebCenter cVSS 3.0 I fality impace	e.com/teo k/securit advisory/	chnetwor y-	A-Ora- Webce/01 -11- 18/155	
CV Scoring Scale (C	VSS)	3-4	ŀ	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	<b>Publish Date</b>	CVSS		Descrip	tion&CVE_	ID	Reference	ce/Patch	NCIIPC ID
- y p = (0)			(CV	ctor: /SS:3.0/AV:N C:L/I:N/A:N) <b>54</b>		•			
Webcenter Site	<u>es</u>								
NA	16-10-2018	4.9	We Ora (su sup 11. vul atta HT We required we sign or We cor We CVS (Coimp (CV)	bcomponent bcomponent ported vers 1.1.8.0. Inerability all acker with TP to cobCenter Site with the vuln bcomplete accomplete accomp	sion M : Advanced ion that is Easily e lows high network a compromise es. Success interaction han the att erability is ites, attac impact essful attac can re ccess to cr access to cr acce	onent of liddleware I UI). The affected is exploitable privileged access via e Oracle ful attacks on from a tacker and in Oracle cks may additional eks of this esult in ritical data all Oracle le data as ate, insert of Oracle ible data. ore 6.9 Integrity Vector: H/UI:R/S:	k/securit advisory,	chnetwor y-	A-0ra- Webce/01 -11- 18/156
Weblogic Serve	1								<u>,                                      </u>
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			chnetwor y- /cpuoct2	A-0ra- Weblo/01- 11-18/157		
CV Scoring Scale (C	<u>-</u>	3-4		4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type Injection; XSS- Cros	(s): CSRF-Cross Site s Site Scripting;	Request F	orgei	y; Dir. TravDi	rectory Traver	sal; DoS-Denia	al of Service;	NA- Not Appli	cable; Sql-SQL

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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-0ra- 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

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(з)			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.tena ble.com/security/ research/tra- 2018-32	A-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-Ora- Weblo/01- 11-18/161

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.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)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	A-0ra- Weblo/01- 11-18/165

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
0 ( )							

Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS (CVSS: J/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 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  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 advisory/cpuoct2 018-4428296.html vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this 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	Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
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 U/C:H/I:H/A:H). CVE-ID:CVE-2018-3197  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. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVS Server Components 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 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S: U/C:H/I:H/A:H). CVE-ID:CVE-2018-	Type(s)			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). <b>CVE-ID:CVE-2018-</b>		
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-	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-	e.com/technetwor k/security- advisory/cpuoct2	Weblo/01-
Prayer Project			7.5	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-	e.com/technetwor k/security- advisory/cpuoct2	Weblo/01-

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Descrip	otion&CVE_	ID	Reference	/Patch	NCIIPC ID
Prayer								
Gain Information	25-10-2018	4.3	Prayer through 1.3.5 sends a Referer https://bugs.n.org/911842 username, when a user clicks on a link in their email because header.t lacks a no-referrer setting. <b>CVE-ID:CVE-2018-18655</b>					A-Pra- Praye/01- 11-18/168
Subrion								
CMS								
XSS	02-10-2018	4.3	_core/admin/p CMS 4.2.1 has parameter. CVE	XSS via the	titles[en]	https://cxs com/issue, 201809026	/WLB-	A-Sub- CMS/01- 11-18/169
	1	Applica	tion,Operating <b>S</b>	System (Ap)	plication,(	OS)		
Canonical,Deb	ian,Libssh							
•	ibssh,Ubuntu L							
NA	17-10-2018	6.4	A vulnerability server-side st versions 0.7.6 a client could crefirst perform resulting in CVE-ID:CVE-20	ate machir and 0.8.4. A eate channe ning autho unauthorize	ne before malicious ls without entication,	https://wv oit- db.com/ex 5638/,http w.libssh.or ity/advisor E-2018- 10933.txt,h usn.ubuntu 795- 2/,https:// obal.sonicv /vuln- detail/SNW 2018- 0016,https ubuntu.com - 1/,https:// ebian.org/s /2018/dsa 4322,https illa.redhat.ow_bug.cgi E-2018- 10933,http s.debian.or	ploits/4 ps://ww rg/secur ries/CV nttps:// n.com/3 /psirt.gl wall.com VLID- :://usn. m/3795 /www.d security :://bugz com/sh i?id=CV	A-Can- Debia/01- 11-18/170
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7 <b>-8</b>	8-9	9-10		
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL									
Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID				Reference	e/Patch	NCIIPC ID
Oracle,Redhat								e/2018/1 010.html, www.rapi lb/modul ary/scan libssh_au	
Enterprise Linu Workstation,JD	ux Desktop,Ente DK,JRE	erprise L	inux	x Server,Ent	erprise Lin	ux Server I	Eus,Enterpi	rise Linux	
NA	16-10-2018	5.1	Emilise Supare Java to una nett pro Java atta from atta add atta resu Emilise Emilise In app typic san app app run con the vull dep	Java SE: 7  a SE Embed exploit authenticate work acc tocols to co a SE En acks require a perso acker and w an Java SE, acks may attional p acks of th alt in takeov bedded. No alies to acally in dboxed alications of alets (in Java untrusted aes from the Java sanda aerability de aloyments, at load and a	aponent of Caponent: sions that an u191, 8u18 ded: 8u182 vulnerability d attacked ess via compromise abedded. e human is on other while the vullava SE E significantly roducts. is vulnerally er of Java Ste: This vulnerally er of Java Ste: This vulnerally er sandboa SE 8), that code (e.g. e internet) a sox for secues not appropries appropries of the process of the p	Dracle Java Hotspot). The affected and 11; bifficult by allows the multiple by Java SE, Successful the Interaction than the linerability bility can bility bility can bility bility can bility bility can bility b	https://a hat.com/s HSA-2018	errata/R 8:2943, ccess.red errata/R 8:3000, ccess.red errata/R 8:3001, ccess.red errata/R 8:3409, ccess.red errata/R 8:3002, ccess.red errata/R 8:3003, ccess.red errata/R 8:3350, ccess.red errata/R	A-0ra- Enter/01- 11-18/175
CV Scoring Scale (CV	VSS)	3-4		4-5	5-6	6-7	7-8	9-10	

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.n etapp.com/adviso ry/ntap- 20181018-0001/, https://usn.ubunt u.com/3804-1/, https://www.debi	
				an.org/security/2 018/dsa-4326	
Enterprise Lin Workstation, J.		erprise l	Linux Server,Enterprise Linux Server E		
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	2018:3003,https://security.netapp.com/advisory/ntap-20181018-0001/,	A-Ora- Enter/01- 11-18/171

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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	https://access.red hat.com/errata/R HSA-2018:2943, https://access.red hat.com/errata/R HSA-2018:3000, https://access.red hat.com/errata/R HSA-2018:3001, https://access.red hat.com/errata/R HSA-2018:3001, https://usn.ubunt u.com/3804-1/, https://www.debi an.org/security/2	
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,	018/dsa-4326 https://access.red hat.com/errata/R HSA-2018:3350, https://access.red hat.com/errata/R HSA-2018:3409, https://security.n	A-0ra- Enter/01- 11-18/172

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
V 1 1 111 m ( ) CODE C C'	ь . п	D' M D'		1000	1 66 1		11 6 1601

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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, https://access.red hat.com/errata/R HSA-2018:3008, https://access.red hat.com/errata/R HSA-2018:3007, https://access.red hat.com/errata/R HSA-2018:3000, https://access.red hat.com/errata/R HSA-2018:2943, https://access.red hat.com/errata/R HSA-2018:2943, https://access.red hat.com/errata/R HSA-2018:2943, https://access.red hat.com/errata/R HSA-2018:2941, https://usn.ubunt u.com/3804-1/, https://www.debi an.org/security/2 018/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.n	A-Ora- Enter/01- 11-18/173

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

Vulnerability Type(s)	<b>Publish Date</b>	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.red hat.com/errata/R HSA-2018:3007, https://access.red hat.com/errata/R HSA-2018:3003, https://access.red hat.com/errata/R HSA-2018:3002, https://access.red hat.com/errata/R HSA-2018:2942, https://access.red hat.com/errata/R HSA-2018:3001, https://access.red hat.com/errata/R HSA-2018:3001, https://access.red hat.com/errata/R HSA-2018:2943, https://access.red hat.com/errata/R HSA-2018:2943, https://access.red hat.com/errata/R HSA-2018:3000, https://access.red hat.com/errata/R HSA-2018:3000, https://usn.ubunt u.com/3804-1/, https://www.debi an.org/security/2 018/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.ubunt u.com/3804-1/, https://security.n etapp.com/adviso ry/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	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
			attacker with network access via	https://www.debi	
			multiple protocols to compromise	an.org/security/2	
			Java SE, Java SE Embedded, JRockit.	018/dsa-4326,	
			While the vulnerability is in Java SE,		
			Java SE Embedded, JRockit, attacks	https://access.red	
			may significantly impact additional	hat.com/errata/R	
			products. Successful attacks of this	HSA-2018:2942	
			vulnerability can result in takeover		
			of Java SE, Java SE Embedded,	,https://access.red	
			JRockit. Note: This vulnerability	hat.com/errata/R	
			applies to Java deployments,	HSA-2018:2943,	
			typically in clients running	https://access.red	
			sandboxed Java Web Start	hat.com/errata/R	
			applications or sandboxed Java	HSA-2018:3003,	
			applets (in Java SE 8), that load and	https://access.red	
			run untrusted code (e.g. code that	hat.com/errata/R	
			comes from the internet) and rely on	HSA-2018:3002	
			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). <b>CVE-ID:CVE-2018-</b>		
			3183		
			Operating System (OS)		

Oracle

Solaris

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)					
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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- Solar/01- 11-18/178

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- Solar/01- 11-18/179

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)  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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- Solar/01- 11-18/182

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

Vulnerability	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- Solar/01- 11-18/184

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

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Type(s)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- Solar/01- 11-18/186

ava i a i cavaa	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CVSS)							

Vulnerability Type(s)	<b>Publish Date</b>	CVSS	Description&CVE_ID	Reference/Patch	NCIIPC ID
Турс(з)			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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- 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.oracl e.com/technetwor k/security- advisory/cpuoct2 018-4428296.html	0-0ra- Solar/01- 11-18/188

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

Vulnerability Type(s)	<b>Publish Date</b>	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		

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