(Moure)	ional Critica Scoring Scale		(Infrastru SVE Repor Jul-31 Jul	t	Protecti		ntre 05 No.14
Vulnerability Type(s)	Publish Date	CVSS		otion & CVE		Reference	/Patch	NCIIPC ID
Application								
Ablgenesistok	en Project							
Ablgenesistoke	n							
Overflow	09-07-2018	5	The mintTo smart contr for ABLG Ethereum to overflow that of the con balance of a any value. CVE-ID:CVE	act impleme enesisToke oken, has an at allows the ntract to s in arbitrary	entation n, an integer e owner set the user to	https://gith m/BlockCh urity/Ether /tree/mast GenesisTok https://gith m/BlockCh urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/ABL een, nub.co ainsSec Tokens eer/GE iint%2	A-Abl- Ablge/01- 08-18/1
Anovabace Pro	oject					10		
Anovabace	<u>.</u>							
Overflow Appletoken Pr	09-07-2018	5	The mintTo smart contr for AnovaB token, has a that allows contract to an arbitrary CVE-ID:CVE	act impleme ace, an Et in integer o the owner set the bal vuser to an	entation hereum werflow of the lance of y value.	https://gith m/BlockCh urity/Ether /tree/mast vaBace, https://gith m/BlockCh urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/Ano nub.co ainsSec Tokens cer/GE iint%2	A-Ano- Anova/01 -08-18/2
Appletoken	ojeci							
Overflow	09-07-2018	5	The mintT smart contr for AppleTo token, has a that allows contract to	oken, an Et in integer o the owner	entation hereum verflow · of the	https://gith m/BlockCh urity/Ether /blob/mast MCHAIN/m 0integer%2	ainsSec Tokens cer/GE aint%2	A-App- Apple/01- 08-18/3
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(Sql-SQL Injection; X	(s): CSRF-Cross Site		orgery; Dir. Trav	7Directory Tr	aversal; Do	S-Denial of Serv	vice; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID
				itrary user to any value. D:CVE-2018-13776		low.md,	,	
						https://github.co m/BlockChainsSec urity/EtherTokens		
						/tree/maste leToken		
Azttoken Proje	ect							
Azttoken					-			
Overflow	09-07-2018	5	The mintTo smart contr for AZTTol token, has a that allows contract to an arbitrary CVE-ID:CVE	act impleme ken, an Et in integer o the owner set the bal vuser to an	entation hereum verflow of the ance of y value.	https://gith m/BlockCha urity/Ether' /tree/maste Token, https://gith m/BlockCha urity/Ether' /blob/maste MCHAIN/m 0integer%2 low.md	ainsSec Fokens er/AZT ub.co ainsSec Fokens er/GE int%2	A-Azt- Aztto/01- 08-18/4
Bcaas Project								
Bcaas	1							
Overflow	09-07-2018	5	The mintTo smart contr for BCaaS, a has an inte allows the contract to an arbitrary CVE-ID:CVE	act impleme in Ethereum eger overflo e owner set the bal v user to an	entation token, ow that of the ance of y value.	https://gith m/BlockCha urity/Ether' /tree/maste aS, https://gith m/BlockCha urity/Ether' /blob/maste MCHAIN/m 0integer%2 low.md	ainsSec Fokens er/BCa ub.co ainsSec Fokens er/GE int%2	A-Bca- Bcaas/01- 08-18/5
Bigcadvancedt								
Bigcadvancedt Overflow	oken 09-07-2018	5		act impleme lvancedTok	entation en, an	https://github.co m/BlockChainsSec urity/EtherTokens		A-Big- Bigca/01- 08-18/6
			Ethereum to	oken, has an	ınteger	/blob/mast	er/GE	
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13759	MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/BIG CAdvancedToken	
Biqutoken Pro	ject				
Biqutoken					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for BiquToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13764	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Biq uToken	A-Biq- Biqut/01- 08-18/7
Bitedutoken P	roject				
Bitedutoken					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for BiteduToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13719	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Bite duToken	A-Bit- Bited/01- 08-18/8
Bitstarti Proje	ct				
Bitstarti					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation	https://github.co m/BlockChainsSec	A-Bit- Bitst/01-
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	(s): CSRF-Cross Site SS- Cross Site Script		orgery; Dir. TravDirectory Traversal; Do	S-Denial of Service; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	EID	Referenc	e/Patch	NCIIPC
			for Bitstarti, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13774				erTokens ster/GE mint%2 o20overf thub.co hainsSec erTokens ster/Bits	08-18/9
Bpstoken Proje Bpstoken	ect							
Overflow	09-07-2018	5	The mintTo smart contra for BpsTok token, has a that allows contract to an arbitrary CVE-ID:CVE	act impleme ten, an Et in integer o the owner set the bal vuser to an	entation hereum verflow of the ance of y value.	https://gi m/BlockC urity/Ethe /tree/mas Token, https://gi m/BlockC urity/Ethe /blob/mas MCHAIN/n 0integer% low.md	hainsSec erTokens ster/Bps thub.co hainsSec erTokens ster/GE mint%2	A-Bps- Bpsto/0 08-18/1
Bsctoken Proje	ect							
Bsctoken								
Overflow	09-07-2018	5	The mintTo smart contra for BSCTok token, has a that allows contract to an arbitrary CVE-ID:CVE	act impleme ten, an Et in integer o the owner set the bal vuser to an	entation hereum verflow of the ance of y value.	https://gi m/BlockC urity/Ethe /tree/mas Token, https://gi m/BlockC urity/Ethe /blob/mas MCHAIN/i 0integer% low.md	hainsSec erTokens ster/BSC thub.co hainsSec erTokens ster/GE mint%2	A-Bsc- Bscto/0 08-18/1
Btpcoin Projec	t							
Btpcoin								
CV Scoring Scale (C)		3-4	4-5	5-6	6-7	7-8	8-9	9-1

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference	/Patch	NCIIPC ID
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for BTPCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13668			https://gith m/BlockCha urity/Ether /tree/maste Coin, https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	A-Btp- Btpco/01- 08-18/12	
Buytoken Proj	ect							
Buytoken Overflow	09-07-2018	5	smart contr for Order Name: Ethereum to overflow that of the con balance of a any value.	oken functio act impleme (ETH) (C BuyToken), oken, has an at allows the ntract to s in arbitrary C-2018-137	ntation ontract an integer owner et the user to	https://gith m/BlockCha urity/Ether /tree/maste Token, https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m	ainsSec Tokens er/Buy ub.co ainsSec Tokens er/GE int%2	A-Buy- Buyto/01 -08- 18/13
						0integer%2 low.md	0overf	
Cartoken Proje	ect							
Cartoken	1					1		
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for CarToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13748https://github.co m/BlockChainsSec Uniteger%20overf low.md,Https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Car Tokenhttps://github.co				A-Car- Carto/01- 08-18/14	
Cerb Coin Proj	ect							
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	(s): CSRF-Cross Site SS- Cross Site Script	-	orgery; Dir. Trav	vDirectory Tra	aversal; Do	oS-Denial of Serv	rice; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Descrip	ption & CVE	ID	Reference	/Patch	NCIIPC ID
Cerb Coin								
Overflow	09-07-2018	5	smart contr for CERB_C token, has a that allows contract to an arbitrary		ntation nereum verflow of the ance of y value.	https://gith m/BlockCha urity/Ether /tree/maste B_Coin, https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/CER nub.co ainsSec Tokens er/GE int%2	A-Cer- Cerb/01- 08-18/15
Cgctoken Proje	ect							
Cgctoken		_						
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for CGCToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13778			https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha urity/Ether /tree/maste Token	A-Cgc- Cgcto/01- 08-18/16	
Cherrycoinfou	ndation Projec	t						
Cherrycoinfour	ndation							
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for CherryCoinFoundation, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13756		https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha urity/Ether /tree/maste rryCoinFou n	ainsSec Tokens er/GE int%2 Ooverf nub.co ainsSec Tokens er/Che	A-Che- Cherr/01 08-18/17	
	•	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
Cjxtoken Proje	ct				
Cjxtoken					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for CJXToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13689	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/CJX Token, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Cjx- Cjxto/01- 08-18/18
Cm Project					
СМ					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for CM, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13714	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/CM, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Cm- CM/01- 08-18/19
Coinquer Proj	ect				
<i>Coinquer</i> Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Coinquer, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13757	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Coi nquer	A-Coi- Coinq/01- 08-18/20

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
	edtoken Proje	ct			
Combilladvand	edtoken				
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for ComBillAdvancedToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13674	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Co mBillAdvancedTo ken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Com- Combi/01 -08- 18/21
Cornerstone P	roject				
Cornerstone	ſ			I	1
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Cornerstone, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13767	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Cor nerstone	A-Cor- Corne/01 -08- 18/22
Crowdnext Pro	oject				
Crowdnext	00.07.2010	-			A C
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Crowdnext (CNX), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13744	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Cro wdnext, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE	A-Cro- Crowd/01 -08- 18/23

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				MCHAIN/mint%2 0integer%20overf low.md	
Cryptosistoker					
<i>Cryptosistoken</i> Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for CryptosisToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13754	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Cry ptosisToken	A-Cry- Crypt/01- 08-18/24
Ctest7 Project	<u> </u>			problerenen	
Ctest7					
Overflow Cws Project	09-07-2018	5	The mint function of a smart contract implementation for CTest7, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13695	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/CTe st7, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Cte- Ctest/01- 08-18/25
CWS Project					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for CWS, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13664	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/CW S, https://github.co m/BlockChainsSec	A-Cws- CWS/01- 08-18/26

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 Script	ing:								

Vulnerability Type(s)	Publish Date	CVSS	Descrij	otion & CVE	ID	Reference	/Patch	NCIIPC ID
			/blob/ma MCHAIN,		urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	er/GE int%2		
Databits Proje	ct							
Databits	00.05.0010	-	m1 t.m	1 6	C	1 //1	,	
Overflow	09-07-2018	5	The mintTo smart contr for Databi token, has a that allows contract to an arbitrary CVE-ID:CVE	act impleme ts, an Et in integer o the owner set the bal v user to any	entation hereum verflow of the ance of y value.	https://gith m/BlockCha urity/Ether /tree/maste abits, https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/Dat ub.co ainsSec Tokens er/GE int%2	A-Dat- Datab/01 -08- 18/27
Destineed Proj	ject		L					
Destineed								
Overflow	09-07-2018 servicetoken P	5	smart contr for Destil Ethereum to overflow the of the con balance of a any value.	smart contract implementation for DestiNeed (DSN), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13699 m/BlockC urity/Ethe https://gi m/BlockC urity/Ethe /blob/mas MCHAIN/m 0integer%		https://gith m/BlockCha urity/Ether /tree/maste tiNeedToke https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/Des n, ub.co ainsSec Tokens er/GE int%2	A-Des- Desti/01- 08-18/28
Deweisecuritys		roject						
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation forhttps://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GEDeWeiSecurityServiceToken, an Ethereum token, has an integer overflow that allowsMCHAIN/mint%2 0integer%20overf				A-Dew- Dewei/01 -08- 18/29	
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type	VSS) (s): CSRF-Cross Site (SS- Cross Site Script	Request F						

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			the owner of the contract to setlow.md,the balance of an arbitraryhttps://github.couser to any value.https://github.coCVE-ID:CVE-2018-13753m/BlockChainsSecurity/EtherTokens/tree/master/DeWeiSecurityServiceToken		
Dinsteincoin P	roject				
Dinsteincoin	I			Ι	
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for DinsteinCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13671	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Din steinCoin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Din- Dinst/01- 08-18/30
Dopnetwork P	roject				
Dopnetwork					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for dopnetwork, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13739	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/dop network, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Dop- Dopne/01 -08- 18/31
Eastcoin Proje	ct				
Eastcoin					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Eastcoin, an Ethereum	https://github.co m/BlockChainsSec urity/EtherTokens	A-Eas- Eastc/01- 08-18/32
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	(s): CSRF-Cross Site SS- Cross Site Script	-	orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13727	/blob/master/GE MCHAIN/mint%2 0integer%20overf low.md,	
				https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/East coin	
Easticoin Proje	ect				
Easticoin	00.05.0010	-		1	A . T
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Easticoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13766	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md,	A-Eas- Easti/01- 08-18/33
				https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/East icoin	
Eddtoken Proj	ect				
Eddtoken	00.07.2010	-		1	
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for eddToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13704	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/edd Token, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Edd- Eddto/01 -08- 18/34
Elearningcoine	· ·				
Elearningcoine Overflow	09-07-2018	5	The mintToken function of a	https://github.co	A-Ele-
CV Scoring Scale (C	-	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	(s): CSRF-Cross Site SS- Cross Site Script	-	orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID						
		smart contract implementation for ELearningCoinERC, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13736	m/BlockChainsSec urity/EtherTokens /tree/master/ELe arningCoinERC, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	Elear/01- 08-18/35						
Entercoin Project Entercoin										
09-07-2018	5	The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterCoin), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13782	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Ent erCoin	A-Ent- Enter/01- 08-18/36						
oject										
09-07-2018	5	The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13735	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Ent erToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Ent- Enter/01- 08-18/37						
	ect 09-07-2018 09ect	o9-07-2018 5 09-07-2018 5 oject 5	09-07-2018 5 The mintToken function of a smart contract implementation for ELearningCoinERC, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. 09-07-2018 5 The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterCoin), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. 09-07-2018 5 09-07-2018 5 The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterCoin), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. 09-07-2018 5 The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. 09-07-2018 5	09-07-2018 5 The mintToken function of a smart contract implementation for ELearningCoinERC, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. https://github.com/BlockChainsSec 09-07-2018 5 The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterCoin), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. https://github.com/BlockChainsSec 09-07-2018 5 The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterCoin), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. https://github.com/BlockChainsSec 09-07-2018 5 The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. https://github.com/BlockChainsSec 09-07-2018 5 The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. https://github.com/BlockChainsSec urity/EtherTokens /tree/master/Ent erToken, overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. https://github.com/BlockChainsSec 09-07-2018						

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 Script	ing;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID F		Reference	/Patch	NCIIPC ID	
Eristicaico								
Overflow	09-07-2018	5	smart contra for Eristica token, has a that allows contract to an arbitrary	oken function act implement ICO, an Ethe an integer ove the owner o set the balan v user to any v 2-2018-13666	tation ereum erflow of the nce of value.	https://gith m/BlockCha urity/Ether /tree/maste ticaICO, https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/Eris ub.co ainsSec Tokens er/GE int%2	A-Eri- Erist/01- 08-18/38
Esh Project								
ESH								
Overflow	09-07-2018	5	smart contra for ESH, ar has an inte allows the contract to an arbitrary	oken function act implement teger overflow e owner of set the balan v user to any v E-2018-13780	https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha urity/Ether /tree/maste	ainsSec Tokens er/GE int%2 Ooverf ub.co ainsSec Tokens	A-Esh- ESH/01- 08-18/39	
Essence Project	:t							
Essence	1							
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Essence, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13702			https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Ess ence, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md		A-Ess- Essen/01- 08-18/40
CV Scoring Scale (C		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				
Exacorecontra	ct Project								
Exacorecontrac	ct								
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for ExacoreContract, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018- 13771	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Exa coreContract	A-Exa- Exaco/01- 08-18/41				
Exsulcoin Project									
Exsulcoin									
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for exsulcoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13683	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/exs ulcoin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Exs- Exsul/01- 08-18/42				
Ffmpeg									
<i>Ffmpeg</i> DoS	05-07-2018	4.3	In FFmpeg 4.0.1, a missing check for failure of a call to init_get_bits8() in the avpriac3_parse_header function in libavcodec/ac3_parser.c may trigger a NULL pointer dereference while converting a crafted AVI file to MPEG4, leading to a denial of service. CVE-ID:CVE-2018-13303	m/FFmpeg/FFmp	A-Ffm- Ffmpe/01 -08- 18/43				
		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. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable;										
Sal-SOL Injection: VSS- Cross Site Script	ina									

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
DoS	05-07-2018	4.3	In FFmpeg 4.0.1, due to a missing check of a profile value before setting it, the ff_mpeg4_decode_picture_head er function in libavcodec/mpeg4videodec.c may trigger a NULL pointer dereference while converting a crafted AVI file to MPEG4, leading to a denial of service. CVE-ID:CVE-2018-13301	https://github.co m/FFmpeg/FFmp eg/commit/2aa90 47486dbff12d9e0 40f917e5f799ed2f d78b	A-Ffm- Ffmpe/01 -08- 18/44
DoS	05-07-2018	4.3	In libavcodec in FFmpeg 4.0.1, improper maintenance of the consistency between the context profile field and studio_profile in libavcodec may trigger an assertion failure while converting a crafted AVI file to MPEG4, leading to a denial of service, related to error_resilience.c, h263dec.c, and mpeg4videodec.c. CVE-ID:CVE-2018-13304	https://github.co m/FFmpeg/FFmp eg/commit/bd27a 9364ca274ca97f1 df6d984e88a0700 fb235	A-Ffm- Ffmpe/01 -08- 18/45
DoS	05-07-2018	5.8	In FFmpeg 4.0.1, an improper argument (AVCodecParameters) passed to the avprirequest_sample function in the handle_eac3 function in the handle_eac3 function in libavformat/movenc.c may trigger an out-of-array read while converting a crafted AVI file to MPEG4, leading to a denial of service and possibly an information disclosure. CVE-ID:CVE-2018-13300	https://www.debi an.org/security/2 018/dsa-4249, https://github.co m/FFmpeg/FFmp eg/commit/95556 e27e2c1d56d9e18 f5db34d6f756f30 11148	A-Ffm- Ffmpe/01 -08- 18/46
DoS	05-07-2018	5.8	In FFmpeg 4.0.1, due to a missing check for negative values of the mquant variable, the vc1_put_blocks_clamped function in libavcodec/vc1_block.c may trigger an out-of-array access	https://github.co m/FFmpeg/FFmp eg/commit/d08d4 a8c7387e758d439 b0592782e4cfa2b 4d6a4	A-Ffm- Ffmpe/01 -08- 18/47

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;										
Cal COL Interstant VCC Course City Carden	·									

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference	/Patch	NCIIPC ID
			information denial of ser	G4, leading disclosure	to an or a			
DoS	05-07-2018	6.8	In FFmpeg 4.0.1, improper handling of frame types (other than EAC3_FRAME_TYPE_INDEPEN DENT) that have multiple independent substreams in the handle_eac3 function in libavformat/movenc.c may trigger an out-of-array access while converting a crafted AVI file to MPEG4, leading to a denial of service or possibly unspecified other impact. CVE-ID:CVE-2018-13302			https://ww an.org/secu 018/dsa-42 https://gith m/FFmpeg, eg/commit, c22216f74c 901f82649e ba50	urity/2 49, nub.co /FFmp /ed22d 75ee7	A-Ffm- Ffmpe/01 -08- 18/48
Finaltoken Pro	oject							
Finaltoken Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for FinalToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13749			https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha urity/Ether /tree/mast lToken	ainsSec Tokens er/GE int%2 Ooverf ub.co ainsSec Tokens	A-Fin- Final/01- 08-18/49
						HUKEII		
Futurxe Projec	ct					HUKEII		
Futurxe Project Futurxe Overflow	ct 09-07-2018	5	smart contra for FuturX token, has a that allows contract to an arbitrary	0	ntation hereum verflow of the ance of v value.	https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md,	ainsSec Tokens er/GE int%2	A-Fut- Futur/01- 08-18/50

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Fut urXe	
Gfcb Project					
Gfcb					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for GFCB, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13670	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/GFC B, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Gfc- Gfcb/01- 08-18/51
	metoken Proje	ct			
Globalsuperga					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for GlobalSuperGameToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13725	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Glo balSuperGameTok en	A-Glo- Globa/01- 08-18/52
Globecoin Proj	ect				
Globecoin	12.07.2010	-			
Overflow	12-07-2018	5	An integer overflow vulnerability exists in the function transfer_tokens_after_ICO of GlobeCoin (GLB), an Ethereum	https://github.co m/VenusADLab/E therTokens/tree/ master/GlobeCoin %28GLB%29,	A-Glo- Globe/01- 08-18/53

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			token smart contract. An attacker could use it to set any user's balance. CVE-ID:CVE-2018-14004	https://github.co m/VenusADLab/E therTokens/blob/ master/SHARKTE CH/SHARKTECH. md	
Gmile Project					
<i>Gmile</i> Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for GMile, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13694	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/GMi le, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Gmi- Gmile/01- 08-18/54
Goldtokenerc2	0 Project				
Goldtokenerc2	0				
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for GoldTokenERC20, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13673	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Gol dTokenERC20, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Gol- Goldt/01- 08-18/55
Gomineworld	Project				
Gomineworld					

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;									

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference	/Patch	NCIIPC ID
Overflow	09-07-2018	5	smart contract implementation for GoMineWorld, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13721			https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha urity/Ether /tree/maste MineWorld	ainsSec Tokens er/GE int%2 Ooverf ub.co ainsSec Tokens	A-Gom- Gomin/01 -08- 18/56
Goochain Proje	ect							
Goochain								
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Goochain, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13677			https://gith m/BlockCha urity/Ether /tree/maste chain, https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	A-Goo- Gooch/01 -08- 18/57	
Greenenergyto	ken Project							
Greenenergyto	ken							
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for GreenEnergyToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13693			https://gith m/BlockCha urity/Ether /tree/maste enEnergyTo https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	A-Gre- Green/01 -08- 18/58	
Hey Project								

nerability Fype(s) Publish Date CVSS		Description & CVE ID	Reference/Patch	NCIIPC ID
09-07-2018	5	The mintToken function of a smart contract implementation for HEY, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13730	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/HEY	A-Hey- HEY/01- 08-18/59
en Project				
r				
	5	The mintToken function of a smart contract implementation for HormitechToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13717	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Hor mitechToken	A-Hor- Hormi/01 -08- 18/60
	_			
09-07-2018	5	The mint function of a smart contract implementation for HYIPCrowdsale1, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13724	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/HYI	A-Hyi- Hyipc/01- 08-18/61
		09-07-2018 5 09-07-2018 5 en Project n 09-07-2018 5 	09-07-2018 5 The mintToken function of a smart contract implementation for HEY, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13730 en Project n 09-07-2018 5 The mintToken function of a smart contract implementation for HormitechToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13717 1 09-07-2018 5 1 09-07-2018 5 1 09-07-2018 5 1 09-07-2018 5 1 09-07-2018 5 1 09-07-2018 5 1 09-07-2018 5 1 09-07-2018 5 1 09-07-2018 5 1 09-07-2018 5 2 1 1 09-07-2018 5 1 1 5 1 1 09-07-2018 5 2 1 1 1 09-07-2018 5 3 1 1 1 <	09-07-2018 5 The mintToken function of a smart contract implementation for HEY, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13730 https://github.com/BlockChainsSecurity/EtherTokens/Liter/HEY 09-07-2018 5 The mintToken function of a smart contract implementation for HormitechToken, an Ethereum token, has an integer https://github.com/BlockChainsSecurity/EtherTokens//tree/master/HEY 09-07-2018 5 The mintToken function of a smart contract implementation for HormitechToken, an Ethereum token, has an integer overflow that allows the owner of the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13717 https://github.com/BlockChainsSecurity/EtherTokens//blob/master/GE 09-07-2018 5 The mint function of a smart ontract implementation for the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13717 https://github.com/BlockChainsSecurity/EtherTokens//tree/master/HormitechToken 09-07-2018 5 The mint function of a smart contract implementation for HYIPCrowdsale1, an Ethereum token, has an integer overflow that allows the owner of the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13717 https://github.com/BlockChainsSecurity/EtherTokens//tree/master/HormitechToken 09-07-2018 5 The mint function of a smart contract implementation for HYIPCrowdsale1, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13724 m/Block

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;									

Vulnerability Type(s)	Publish Date	CVSS	Descrij	ption & CVE	ID	Reference/	Patch	NCIIPC ID	
Hyiptoken Proj	iect								
Hyiptoken	,								
Overflow	09-07-2018	5	contract ir HYIPToken, token, has a that allows contract to an arbitrary	unction of a nplementati an integer o the owner set the bal user to any 5-2018-137	on for hereum verflow of the ance of y value.	https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%2 low.md, https://gith m/BlockCha urity/Ether /tree/maste PToken	ainsSec Tokens er/GE int%2 Ooverf ub.co ainsSec Tokens	A-Hyi- Hyipt/01- 08-18/62	
Ico Dollar Proj	ect								
Ico Dollar									
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for ICO Dollar (ICOD), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13686			https://gith m/BlockCha urity/Ether' /tree/maste Dollar, https://gith m/BlockCha urity/Ether' /blob/maste MCHAIN/mi 0integer%2 low.md	A-Ico- Ico/01- 08-18/63		
Ideacoin Proje	ct								
Ideacoin	0.0.07.07.17							A-Ide-	
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for IdeaCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13706			m/BlockCha urity/Ether' /tree/maste Coin,https:/ b.com/Block sSecurity/Et kens/blob/n /GEMCHAIN	m/BlockChainsSec urity/EtherTokens /tree/master/Idea Coin,https://githu b.com/BlockChain sSecurity/EtherTo kens/blob/master /GEMCHAIN/mint %20integer%20ov		
		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
Instacocoa Pro	viect				
Instacocoa	<u>,</u>				
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Instacocoa, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13690	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Inst acocoa, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Ins- Insta/01- 08-18/65
Ipmcoin Proje	ct				
Ipmcoin					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for IPMCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13700	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/IPM Coin	A-Ipm- Ipmco/01 -08- 18/66
Iseevoicetokei	n Project				
Iseevoicetoken					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for ISeeVoiceToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13726	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens	A-Ise- Iseev/01- 08-18/67

CV Scoring Scale (CVSS)	3-4	4-5	5-0	0-7	7-0	0-9	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;										

= <

4 5

0.4

		Description & CVE ID	Reference/Patch	NCIIPC ID							
			/tree/master/ISee VoiceToken								
oject											
Jeanstoken											
09-07-2018	5	The mintToken function of a smart contract implementation for JeansToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13769	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md,	A-Jea- Jeans/01- 08-18/68							
			m/BlockChainsSec urity/EtherTokens /tree/master/Jean sToken								
oject											
1											
09-07-2018	5	The mintToken function of a smart contract implementation for JiucaiToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13783	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md,	A-Jiu- Jiuca/01- 08-18/69							
			https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Jiuc aiToken								
ct											
-											
09-07-2018	5	The mintToken function of a smart contract implementation for JixoCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13728	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md,	A-Jix- Jixoc/01- 08-18/70							
	ct	09-07-2018 5 oject 09-07-2018 5 09-07-2018 5 i i i i i i i i i i i i i i i i i i i	09-07-2018 5 The mintToken function of a smart contract implementation for JeansToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13769 09-07-2018 5 The mintToken function of a smart contract implementation for JiucaiToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13769 09-07-2018 5 The mintToken function of a smart contract implementation for JiucaiToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13783 09-07-2018 5 The mintToken function of a smart contract implementation for JixoCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13783	09-07-2018 5 The mintToken function of a smart contract implementation for JeansToken, an Ethereum Utken, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13769 https://github.com/BlockChainsSecurity/EtherTokens/Utee/master/Jean/Stoken 09-07-2018 5 The mintToken function of a smart contract implementation for JiucaiToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of JucaiToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of JucaiToken an arbitrary user to any value. CVE-ID:CVE-2018-13783 https://github.com/BlockChainsSecurity/EtherTokens/Itee/master/Jean/Stoken 09-07-2018 5 The mintToken function of a smart contract implementation for JiucaiToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of JucaiToken strity/EtherTokens/Itee/master/JiucaiToken 09-07-2018 5 The mintToken function of a smart contract implementation for JiucaiToken function of a smart contract to set the balance of Utee/master/JiucaiToken 09-07-2018 5 The mintToken function of a smart contract implementation for JiucaiToken for JiucaiToken function of a smart contract to set the balance of Utee/master/GE https://github.com/BlockChainsSecurity/EtherTokens/Itee/master/JiucaiToken							

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;									

		Description & CVE ID	Reference/Patch	NCIIPC ID
			m/BlockChainsSec urity/EtherTokens /tree/master/Jixo Coin	
ject				
09-07-2018	5	The mintToken function of a smart contract implementation for JPMD100B, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13729	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/JPM D100B	A-Jpm- Jpmd1/01 -08- 18/71
ject				
09-07-2018	5	The mintToken function of a smart contract implementation for JustWallet, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13751	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co	A-Jus- Justw/01- 08-18/72
			m/BlockChainsSec urity/EtherTokens /tree/master/Just Wallet	
09-07-2018	5	The mintToken function of a smart contract implementation for kBit, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/kBit , https://github.co m/BlockChainsSec	A-Kbi- Kbit/01- 08-18/73
	•ject 09-07-2018 ject ject 09-07-2018 09-07-2018 09-07-2018 09-07-2018	09-07-2018 5 ject 09-07-2018 5	09-07-2018 5 The mintToken function of a smart contract implementation for JPMD100B, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13729 ject 09-07-2018 5 The mintToken function of a smart contract implementation for JustWallet, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13729 09-07-2018 5 The mintToken function of a smart contract implementation for JustWallet, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13751 09-07-2018 5 The mintToken function of a smart contract implementation for kBit, an Ethereum token, has an integer overflow that allows the owner of the contract implementation for kBit, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.	09-07-2018 5 The mintToken function of a smart contract implementation for JPMD100B, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13729 https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GE 09-07-2018 5 The mintToken function of a smart contract implementation for JustWallet, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13729 https://github.com/BlockChainsSecurity/EtherTokens/tree/master/JPM D100B ject 09-07-2018 5 The mintToken function of a smart contract implementation for JustWallet, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13751 m/BlockChainsSecurity/EtherTokens/blob/master/GE 09-07-2018 5 The mintToken function of a smart contract implementation for JustWallet, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of m/BlockChainsSecurity/EtherTokens/tust/Wallet 09-07-2018 5 The mintToken function of a smart contract implementation for kBit, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of m/BlockChainsSecurity/EtherTokens/tree/master/Just Wallet

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Descrij	otion & CVE	ID	Reference	/Patch	NCIIPC II
			CVE-ID:CVE-2018-13746			urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	er/GE int%2	
Kissme Projec	t							
Kissme	00.07.0040	-	m1		C	1	,	A 17
Overflow	09-07-2018	5	smart contr for KissMe, a has an inte allows the contract to an arbitrary	oken functio act impleme an Ethereum eger overflo e owner o set the bala user to any C-2018-137 0	ntation token, w that of the ance of v value.	https://gith m/BlockCha urity/Ether /tree/maste Me, https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/Kiss ub.co ainsSec Tokens er/GE int%2	A-Kis- Kissm/0 -08- 18/74
Landcoin Proj	ect							
Landcoin	Γ							
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Antoken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13720			https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha	ainsSec Tokens er/GE int%2 0overf ub.co ainsSec	A-Lan- Landc/02 -08- 18/75
						urity/Ether /tree/maste oken		
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for LandCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13765			https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md,	ainsSec Tokens er/GE int%2 Ooverf	A-Lan- Landc/02 -08- 18/76
		3-4	4-5	5-6	6-7	https://gith	ub.co 8-9	9-10
CV Scoring Scale (C	VSS)	5-4	T J	3-0	0-7	1.0	0-9	710

Vulnerability Type(s)	Publish Date	CVSS	Descrip	tion & CVE	ID	Reference/	Patch	NCIIPC ID
						m/BlockCha urity/Ether /tree/maste dCoin	Гokens	
Lexittoken Pro	ject							
Lexittoken								
Overflow	09-07-2018	5	The mintT smart contra for LexitTo token, has a that allows contract to an arbitrary CVE-ID:CVE	ken, an Et n integer o the owner set the bal user to an	entation hereum verflow of the ance of y value.	https://gith m/BlockCha urity/Ether /tree/maste tToken, https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md	insSec Fokens r/Lexi ub.co insSec Fokens er/GE int%2	A-Lex- Lexit/01- 08-18/77
Lolicoin Projec	t							
Lolicoin								
Overflow Lottery Project	09-07-2018	5	The mintT smart contra for LoliCoi token, has a that allows contract to an arbitrary CVE-ID:CVE	n, an Et n integer o the owner set the bal user to an	entation hereum verflow of the ance of y value.	https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md, https://gith m/BlockCha urity/Ether /tree/maste Coin	iinsSec Fokens er/GE int%2 Doverf ub.co iinsSec Fokens	A-Lol- Lolic/01- 08-18/78
Lottery								
Overflow	09-07-2018	5	The mintT smart contra for Lotter token, has a that allows contract to an arbitrary	y, an Et n integer o the owner set the bal	entation hereum verflow of the ance of	https://gith m/BlockCha urity/Ether /tree/maste ery, https://gith	insSec Γokens er/Lott	A-Lot- Lotte/01- 08-18/79
CV Scoring Scale (CV	755)	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. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable;										
Sql-SQL Injection; XSS- Cross Site Script	ing;									

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference	/Patch	NCIIPC ID
			CVE-ID:CVE	5-2018-136	78	m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	Tokens er/GE int%2	
Malaysia Coins	•							
<u>Malaysia Coins</u> Overflow	12-07-2018	5	vulnerabilit function	y exists i transferAny coins (Xmo token attacker co ny user's b	y of c), an smart uld use palance.	https://gith m/VenusAI therTokens master/Mal %20coins% %29, https://gith m/VenusAI therTokens master/SHA CH/SHARK md	DLab/E /tree/ laysia 528Xmc ub.co DLab/E /blob/ ARKTE	A-Mal- Malay/01 -08- 18/80
Malltoken Proj	ect					ma		
Malltoken								
Overflow	09-07-2018	5	smart contra for MallTol token, has a that allows contract to an arbitrary	The mintToken function of a smart contract implementation for MallToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13688		https://gith m/BlockCha urity/Ether /tree/maste Token, https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/Mall nub.co ainsSec Tokens er/GE int%2	A-Mal- Mallt/01- 08-18/81
Mehditazitoke								
Mehditazitoker Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for MehdiTAZIToken, an Ethereum token, has an integer overflow that allows the ownerhttps://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Meh diTAZIToken,				A-Meh- Mehdi/01 -08- 18/82	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13692	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
Mjolnir Projec	t				
<i>Mjolnir</i> Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Mjolnir, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13710	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Mjol nir, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Mjo- Mjoln/01- 08-18/83
Moneychainne	t Project				
Moneychainne	t				
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for MoneyChainNet (MCN), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13760	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Mon eyChainNetToken	A-Mon- Money/0 1-08- 18/84
Mp3 Coin Proje	ect				
Mp3 Coin					
Overflow	12-07-2018	5	An integer overflow vulnerability exists in the function distribute of MP3	https://github.co m/VenusADLab/E therTokens/tree/	A-Mp3- Mp3/01- 08-18/85
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
Vulnerability Type(Sql-SQL Injection; X			orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Coin (MP3), an Ethereum token smart contract. An attacker could use it to set any user's balance. CVE-ID:CVE-2018-14002	master/MP3%20C oin%28MP3%29, https://github.co m/VenusADLab/E therTokens/blob/ master/SHARKTE CH/SHARKTECH. md	
Myylc Project					
<i>Myylc</i> Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for MyYLC, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13781	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/MyY LCToken	A-Myy- Myylc/01- 08-18/86
Ncu Project					
NCU Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for NCU, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13669	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf	A-Ncu- NCU/01- 08-18/87
Neo Genesis To	oken Project			low.md	
Neo Genesis To	ken				

CV Scoring Scale (CVSS)	3-4	4-5	5-0	0-7	/-0	0-9	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 Script	ing;								

. .

0 4

= <

Т

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID
Overflow	12-07-2018	5	vulnerability function m Neo Genesi Ethereum contract. An it to set a CVE-ID:CVE	y exists ultipleTrans s Token (N token attacker co ny user's b	GT), an smart uld use palance.	https://gith m/VenusAD therTokens/ master/Neo enesis%20T %28NGT%2 https://gith m/VenusAD therTokens/ master/SHA CH/SHARKT md	Lab/E /tree/ %20G oken 29, ub.co Lab/E /blob/ .RKTE	A-Neo- Neo/01- 08-18/88
Netkilleradvar			ect					
Netkilleradvan						, , , , ,	, ,	
Overflow	09-07-2018	5	The mintT smart contr for NetkillerAdy op, an Ether integer ove the owner o the balance user to any CVE-ID:CVE	vancedToke reum token, erflow that f the contrace of an an value.	ntation nAirDr has an allows ct to set bitrary	https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md, https://gith m/BlockCha urity/Ether /tree/maste killerAdvanc kenAirDrop	iinsSec Fokens er/GE int%2 Ooverf ub.co iinsSec Fokens er/Net	A-Net- Netki/01- 08-18/89
Netkillertoken	Project		I		I	•		
Netkillertoken								
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Enterprise Token Ecosystem (ETE) (Contract Name: NetkillerToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13773			https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md, https://gith m/BlockCha urity/Ether /tree/maste	insSec Fokens er/GE int%2 Ooverf ub.co iinsSec Fokens	A-Net- Netki/01- 08-18/90
		3-4	4-5	5-6	6-7	killerToken	8-9	9-10
CV Scoring Scale (C		5-4	4-5	3-0	0-7	/-0	0-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Normikaivo Pr	oject				
Normikaivo					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for normikaivo, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13687	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/nor mikaivo, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Nor- Normi/01 -08- 18/91
Obtcoin Project	:t				
Obtcoin					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for OBTCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13672	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/OBT Coin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Obt- Obtco/01- 08-18/92
Onechain Proj	ect				
Onechain				.	
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for OneChain, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13740	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/One Chain, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2	A-One- Onech/01 -08- 18/93

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

Vulnerability Type(s)	Publish Date	CVSS	Descrip	tion & CVE	ID	Reference/Pat	ch	NCIIPC ID
						0integer%20ove low.md	erf	
Oracle								
Agile Product L	ifecycle Manag.	ement I	For Process					
NA	18-07-2018	4	Vulnerabili Agile Pr Managemen component Chain I (subcompor The suppor affected is exploitable allows high with networ to compron Product Life for Process. of this vulne	t for of Oracle Products ent: Insta- ted version 6.2.0.0. vulne privileged a ck access vi nise Oracle cycle Mana Successful erability can ized read ac of Oracle ecycle Mana accessible Base Sco lity impacts V:N/AC:L/F I:N/A:N).	ifecycle Process Supply Suite Ilation). that is Easily trability ttacker a HTTP e Agile gement attacks n result ccess to Agile gement e data. re 2.7 s). CVSS PR:H/UI	NA		A-Ora- Agile/01- 08-18/94
Applications M					a 1			
NA	18-07-2018	5	Applications component Business (subcompor Diagnostics Supported affected an 12.2.4, 12 12.2.7. Ex vulnerability unauthentic network ac compromise	of Orac ent: versions the versions the versions the versions the versions the versions the versions of the version	fanager cle E- Suite Oracle orfaces). nat are 12.2.3, 6 and loitable allows er with TTP to Oracle	NA 7.8	8.9	A-Ora- Appli/01- 08-18/95
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type	-	-	orgery; Dir. Trav	vDirectory Tra	aversal; Do	S-Denial of Service; N	A- No	t Applicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			ApplicationsManager.Successful attacks of thisvulnerability can result inunauthorized access to criticaldata or complete access to allOracle Applications Manageraccessible data. CVSS 3.0 BaseScore 7.5 (Confidentialityimpacts).CVSSVector:(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).CVE-ID:CVE-2018-2996		
Banking Corpo	rate Lending				
DoS	18-07-2018	5.5	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Corporate Lending. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:L). CVE-ID:CVE-2018-3042	NA	A-Ora- Banki/01- 08-18/96
DoS	18-07-2018	6.5	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial	NA	A-Ora- Banki/01- 08-18/97

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;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Corporate Lending. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:L). CVE-ID:CVE-2018-3036		
NA	18-07-2018	3.5	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can	NA	A-Ora- Banki/01- 08-18/98

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;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID			Reference/	NCIIPC ID	
			result in un to critical access to a Corporate I data. CVSS (Confidentia Vector: (CVSS:3.0/A :N/S:U/C:H/ CVE-ID:CVE	data or co Ill Oracle H Lending aco 3.0 Base Sc Ility impacts V:N/AC:H/I 'I:N/A:N).	omplete Banking cessible ore 5.3 6). CVSS PR:L/UI			
NA	18-07-2018	4		ty in the orporate I of Oracle Finance Appli- nent: Core m versions the re 12.3.0, 0 and 14.1.0 vulne privileged a rk access vi ise Oracle I dending. Sup is vulnerable nauthorized hang or fre crash (co Oracle I Lending. CV 6.5 (Ava CVSS V:N/AC:L/F (1:N/A:H).	Oracle Lending inancial ications nodule). nat are 12.4.0, D. Easily erability ettacker a HTTP Banking ccessful ility can ability quently omplete Banking /SS 3.0 ilability Vector: PR:L/UI	NA		A-Ora- Banki/01- 08-18/99
NA	18-07-2018	4.9	Vulnerabili Banking C component Services (subcompor Supported affected ar 12.5.0, 14.0. exploitable allows low	of Oracle Fi Appl ent: Core m versions th e 12.3.0, 0 and 14.1.0 vulne	Lending inancial ications nodule). nat are 12.4.0,). Easily erability	NA		A-Ora- Banki/01- 08- 18/100
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
			with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Corporate Lending, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-3048		
NA	18-07-2018	5	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 5.3	NA	A-Ora- Banki/01- 08- 18/101

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Descrip	tion & CVE	ID	Reference/	Patch	NCIIPC ID
			(Confidentia Vector: (CVSS:3.0/A :N/S:U/C:L/I CVE-ID:CVE	V:N/AC:L/F I:N/A:N).	PR:N/UI			
NA	18-07-2018	5.5	Vulnerabilit Banking Co component of Services (subcomponent Supported of affected ar 12.5.0, 14.0.0 exploitable allows low p with networ to comprom Corporate L attacks of the result in creation, modification data or all Corporate I data as wel access to complete ac Banking Co accessible da Score 8.1 (O Integrity Vector: (CVSS:3.0/AT :N/S:U/C:H/	ty in the orporate 1 of Oracle F Appl ent: Core n versions the e 12.3.0, 0 and 14.1.0 vulne privileged a k access vi ise Oracle 1 ending. Su is vulnerable unaut deletion access to l Oracle 1 cending acc l as unaut critical d critical d critic	Oracle Lending inancial ications nodule). nat are 12.4.0, D. Easily erability attacker a HTTP Banking ccessful ility can horized or critical Banking cessible horized ata or Oracle Lending 0.0 Base ity and CVSS PR:L/UI 0	NA		A-Ora- Banki/01- 08- 18/102
NA	18-07-2018	5.5	Vulnerabilit Banking Co component of Services (subcompon Supported or affected ar 12.5.0, 14.0.0 exploitable	orporate 1 of Oracle F Appl ent: Core n versions tl e 12.3.0, 0 and 14.1.0	Lending inancial ications nodule). nat are 12.4.0,	NA		A-Ora- Banki/01- 08- 18/103
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type	-	Request F	orgery; Dir. Trav	-Directory Tr	aversal; DoS	-Denial of Servi	ice; NA- No	ot Applicable;

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N). CVE-ID:CVE-2018-3044		
NA	18-07-2018	5.8	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Corporate Lending, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending	NA	A-Ora- Banki/01- 08- 18/104

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending 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-2018-2895		
Banking Paym					
DoS	18-07-2018	5.5	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Payments. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:L). CVE-ID:CVE-2018-3023	NA	A-Ora- Banki/01- 08- 18/105
DoS	18-07-2018	6.5	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported	NA	A-Ora- Banki/01- 08- 18/106

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Payments. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:L). CVE-ID:CVE-2018-3020		
NA	18-07-2018	3.5	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Payments accessible data. CVSS 3.0 Base	NA	A-Ora- Banki/01- 08- 18/107

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Servi	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:H/I:N/A:N). CVE-ID:CVE-2018-3025		
NA	18-07-2018	4	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Payments. 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-2018-3022	NA	A-Ora- Banki/01- 08- 18/108
NA	18-07-2018	4.9	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the	NA	A-Ora- Banki/01- 08- 18/109

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			attacker and while the vulnerability is in Oracle Banking Payments, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-3026		
NA	18-07-2018	5	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Banking Payments 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-2018-3021	NA	A-0ra- Banki/01- 08- 18/110

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;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	5.5	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Payments accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Payments 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-2018-3027	e Financial Services ons (subcomponent: s Core). Supported that are affected are 2.3.0, 12.4.0, 12.5.0 .0. Easily exploitable lity allows low d attacker with access via HTTP to ise Oracle Banking s. Successful attacks ilnerability can result uthorized creation, or modification access il data or all Oracle Payments accessible well as unauthorized o critical data or access to all Oracle Payments accessible S 3.0 Base Score 8.1 attality and Integrity CVSS Vector: /AV:N/AC:L/PR:L/UI EH/I:H/A:N).	
NA	18-07-2018	5.5	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	NA	A-Ora- Banki/01- 08- 18/112

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N). CVE-ID:CVE-2018-3024		
NA	18-07-2018	5.8	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Payments, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments 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).	NA	A-Ora- Banki/01- 08- 18/113

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2896		
Business Intell	igence Publishe	r			
NA	18-07-2018	4	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Web Server). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher 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-2018-2925	NA	A-Ora- Busin/01- 08- 18/114
NA	18-07-2018	6.4	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all BI Publisher accessible data as well as unauthorized read	NA	A-Ora- Busin/01- 08- 18/115

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
	10.07.2010	6.4	access to a subset of BI Publisher 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 :N/S:U/C:L/I:H/A:N). CVE-ID:CVE-2018-2958		A Ora
NA	18-07-2018	6.4	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Layout Tools). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all BI Publisher accessible data as well as unauthorized read access to a subset of BI Publisher 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 :N/S:U/C:L/I:H/A:N). CVE-ID:CVE-2018-2900	NA	A-Ora- Busin/01- 08- 18/116
	ss Managemen				
NA	18-07-2018	6.4	Vulnerability in the OracleBusiness Process ManagementSuite component of OracleFusionMiddleware(subcomponent:ProcessAnalysis& Discovery).Supported versions that areaffectedare11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0and12.2.1.3.0.Easily	NA	A-Ora- Busin/01- 08- 18/117

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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Process Management Suite. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Business Process Management Suite accessible data as well as unauthorized access to critical data or complete access to all Oracle Business Process Management Suite accessible data. CVSS 3.0 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :N/S:U/C:H/I:H/A:N). CVE-ID:CVE-2018-3100		
Communication NA	ns Convergence 18-07-2018	5.8	Vulnerability in the Oracle	NA	A-Ora-
			Communications Messaging Server component of Oracle Communications Applications (subcomponent: Web Client). The supported version that is affected is 3.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Messaging Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Messaging Server, attacks may significantly impact additional		Commu/0 1-08- 18/118

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Servi	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Messaging Server accessible data as well as unauthorized read access to a subset of Oracle Communications Messaging 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-2018-2936		
Communicatio	ns Eagle Local N	Number	Portability Application Process)r	
NA	18-07-2018	6.4	Vulnerability in the Oracle Communications EAGLE LNP Application Processor component of Oracle Communications Applications (subcomponent: GUI). The supported version that is affected is 10.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications EAGLE LNP Application Processor. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications EAGLE LNP Application Processor accessible data as well as unauthorized read access to a subset of Oracle Communications EAGLE LNP Application Processor accessible data as well as unauthorized read access to a subset of Oracle Communications EAGLE LNP Application Processor accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and	NA	A-Ora- Commu/0 1-08- 18/119

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-2904		
Customer Rela	tionship Manag	lement '	Technical Foundation		
NA	18-07-2018	5.8	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E- Business Suite (subcomponent: Preferences). 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 CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, 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 CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation 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-2018-2993	NA	A-Ora- Custo/01- 08- 18/120

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Database Serv	18-07-2018	5.8	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E- Business Suite (subcomponent: Preferences). 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 CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, 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 CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation 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-2018-3017	NA	A-Ora- Custo/01- 08- 18/121
NA	18-07-2018	3.5	Vulnerability in the Java VM	NA	A-Ora-
	10-07-2018	5.5	component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2,12.2.0.1 and 18.2.	INA	A-014- Datab/01 -08- 18/122
		3.4	4-5 5-6 6-7	7.8 8.9	9.10

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java VM accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:H/I:N/A:N). CVE-ID:CVE-2018-3004		
NA	18-07-2018	3.6	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.1 and 18.2. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Core RDBMS accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Core RDBMS. CVSS 3.0 Base Score 8.4 (Integrity and Availability	NA	A-Ora- Datab/01 -08- 18/123

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID
			impacts). (CVSS:3.0/A N/S:C/C:N/I CVE-ID:CVE	V:L/AC:L/P I:H/A:H).				
E-business Suit	te							
NA	18-07-2018	5	Application component Business (subcompor / File Uploa version that	of Orac nent: Attac ad). The sup at is affect asily exp y ated attack cess via H e Object 1 attacks of y can res d update, in s to some of Object lata. CVSS 3 Integrity in V:N/AC:L/F (I:L/A:N).	Library cle E- Suite hments oported cted is loitable allows er with TTP to Oracle Library. of this sult in nsert or f Oracle Library 0.0 Base npacts). Vector: PR:N/UI	NA		A-Ora-E- bus/01- 08- 18/124
Enterprise Mai	nager Ops Cente	er					I	
NA	18-07-2018	6.4	VulnerabilityintheNAEnterpriseManagerOpsCentercomponentofCentercomponentofSuite(subcomponent:Networking).Thesupportedversionversionthatisaffectedsiteis12.2.2.EasilyexploitablevulnerabilityallowsunauthenticatedattackerunauthenticatedEnterpriseManagerOpsCenter.Successfulattacksattacksofthis					A-Ora- Enter/01- 08- 18/125
CV Scoring Scale (CV	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

 Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability can result in unauthorized access to critical data or complete access to all Enterprise Manager Ops Center accessible data as well as unauthorized update, insert or delete access to some of Enterprise Manager Ops Center 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 :N/S:U/C:H/I:L/A:N). CVE-ID:CVE-2018-2976		
	-		eral Management		
DoS	18-07-2018	5.5	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Enterprise Limits and Collateral Management.	NA	A-Ora- Flexc/01- 08- 18/126

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:L). CVE-ID:CVE-2018-3043		
DoS	18-07-2018	6.5	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as du unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Enterprise Limits and Collateral Management. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:L). CVE-ID:CVE-2018-3037	NA	A-Ora- Flexc/01- 08- 18/127

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	3.5	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:H/I:N/A:N). CVE-ID:CVE-2018-3047	NA	A-Ora- Flexc/01- 08- 18/128
NA	18-07-2018	4	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management.	NA	A-Ora- Flexc/01- 08- 18/129

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;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle FLEXCUBE Enterprise Limits and Collateral Management. 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-2018-3041		
NA	18-07-2018	4.9	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Enterprise Limits and Collateral Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management	NA	A-Ora- Flexc/01- 08- 18/130

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-3049		
NA	18-07-2018	5	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management 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-2018-3039	NA	A-Ora- Flexc/01- 08- 18/131
NA	18-07-2018	5.5	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent:	NA	A-Ora- Flexc/01- 08- 18/132

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

NA18-07-20185.5Vulnerability and Collateral ManagementNA18-07-20185.5NA18-07-20185.5Vulnerability in the Oracle FLEXCUBE Collateral CollateralNAA-Orac A-Orac	Vulnerability Type(s)	Publish Date	CVSS	Descri	ption & CVE	ID	Reference	/Patch	NCIIPC ID
and Collateral Management. Successful attacks of this		18-07-2018	5.5	versions th 12.3.0, 14.0 exploitable allows low with netwo to com FLEXCUBE and Collat Successful vulnerabilit unauthoriz deletion or to critical FLEXCUBE and Colla accessible unauthoriz data or con Oracle FLI Limits Managemen CVSS 3.0 (Confidenti impacts). (CVSS:3.0/A :N/S:U/C:H CVE-ID:CV Vulnerabil FLEXCUBE and Colla component Services (subcompo Infrastructor versions th 12.3.0, 14.0 exploitable allows low with netwo	at are affect .0 and 14.1.0 vulne privileged a rk access vi promise Enterprise teral Mana attacks of y can reserved comodification data or all Enterprise teral Mana data as we ed access to nplete access EXCUBE En- and Como the accessible Base Sco ality and IS CVSS AV:N/AC:L/H /I:H/A:N). E-2018-305 ity in the Enterprise teral Mana of Oracle F Appl nent: ure). Sup at are affect .0 and 14.1.0 privileged a rk access vi promise Enterprise teral Mana	ted are b. Easily erability attacker a HTTP Oracle Limits gement. of this sult in reation, access Oracle Limits gement vell as critical ss to all terprise ollateral e data. re 8.1 ategrity Vector: PR:L/UI 1 Oracle Limits gement inancial ications pported ted are 0. Easily erability attacker a HTTP Oracle Limits gement	NA		A-Ora- Flexc/01- 08- 18/133
CV Scoring Scale (CVSS) 3-4 4-5 5-6 6-7 7-8 8-9 9-6	CV Scoring Scale (C	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
			vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N). CVE-ID:CVE-2018-3045		
NA	18-07-2018	5.8	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Enterprise Limits and Collateral Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or	NA	A-Ora- Flexc/01- 08- 18/134

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	-Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral 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-2018-2897		
Flexcube Inves					
DoS	18-07-2018	5.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Investor Servicing. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:L).	NA	A-Ora- Flexc/01- 08- 18/135

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-3031		
DoS	18-07-2018	6.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Investor Servicing. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:L).	NA	A-Ora- Flexc/01- 08- 18/136
NA	18-07-2018	3.5	CVE-ID:CVE-2018-3028Vulnerability in the OracleFLEXCUBE Investor Servicingcomponent of Oracle FinancialServicesApplications(subcomponent:Infrastructure).Supportedversions that are affected are12.0.4, 12.1.0, 12.3.0 and12.4.0.Difficultto exploit	NA	A-Ora- Flexc/01- 08- 18/137

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:H/I:N/A:N). CVE-ID:CVE-2018-3033		
NA	18-07-2018	4	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle FLEXCUBE Investor Servicing. 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-2018-3030	NA	A-Ora- Flexc/01- 08- 18/138
NA	18-07-2018	4.9	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial	NA	A-Ora- Flexc/01- 08-

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;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Investor Servicing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-3034		18/139
NA	18-07-2018	5	Vulnerability in the OracleFLEXCUBE Investor Servicingcomponent of Oracle FinancialServicesApplications(subcomponent:Infrastructure).Supportedversions that are affected are12.0.4,12.1.0,12.4.0.Easilyexploitablevulnerabilityallowsunauthenticated attacker with	NA	A-Ora- Flexc/01- 08- 18/140

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	-Directory Tr	aversal; DoS-	Denial of Servi	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing 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-2018-3029		
NA	18-07-2018	5.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing 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-2018-3035	NA	A-Ora- Flexc/01- 08- 18/141

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	5.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N). CVE-ID:CVE-2018-3032	NA	A-Ora- Flexc/01- 08- 18/142
NA	18-07-2018	5.8	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human	NA	A-Ora- Flexc/01- 08- 18/143

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Investor Servicing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing 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-2018-2898		
Flexcube Unive DoS	18-07-2018	5.5	Vulnerability in the Oracle	NA	A-Ora- Fleyc/01-
			FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a		Flexc/01- 08- 18/144

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 Script	ing;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:L). CVE-ID:CVE-2018-2980		
DoS	18-07-2018	6.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:L). CVE-ID:CVE-2018-2974	NA	A-Ora- Flexc/01- 08- 18/145

	CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10			
Sal-SAL Injection: XSS- Cross Site Scripting:	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)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	3.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:H/I:N/A:N). CVE-ID:CVE-2018-2982	NA	A-Ora- Flexc/01- 08- 18/146
NA	18-07-2018	4	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in	NA	A-0ra- Flexc/01- 08- 18/147

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 Script	ing;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle FLEXCUBE Universal Banking. 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-2018-2979		
NA	18-07-2018	4.9	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector:	NA	A-Ora- Flexc/01- 08- 18/148

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;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-3019		
NA	18-07-2018	5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking 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-2018-2975	NA	A-Ora- Flexc/01- 08- 18/149
NA	18-07-2018	5.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking.	NA	A-Ora- Flexc/01- 08- 18/150

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;								
sqr-sqL injection; Ass- cross site scripting;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking 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-2018-3015		
NA	18-07-2018	5.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector:	NA	A-Ora- Flexc/01- 08- 18/151

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;									

Vulnerability Type(s)	Publish Date	CVSS	Descrip	tion & CVE	ID	Reference	/Patch	NCIIPC ID
			(CVSS:3.0/A :N/S:U/C:L/ CVE-ID:CVE	I:L/A:N).	,			
NA	18-07-2018	5.8	Vulnerabili FLEXCUBE component Services (subcomponent Infrastructur versions that 11.3.0, 11.4 12.0.3, 12.1 12.4.0, 14.0.4 exploitable allows attacker wite via HTTP Oracle FLE Banking. S require hu from a pers attacker at vulnerability FLEXCUBE	ty in the Universal I of Oracle Finants Appli- ent: re). Sup at are affect and 14.1.0 vulne unauther th network to comp XCUBE Un uccessful uman inter on other the and while vis in Universal B nay signi ditional pri attacks of v can res d update, in s to some o Universal I data as v d read acce Oracle FLE anking acce 3.0 Base Sc lity and In CVSS V:N/AC:L/F f:L/A:N).	Oracle Banking inancial ications oported ted are 12.0.2, 12.3.0, 0. Easily erability nticated access oromise niversal attacks eraction nan the e the Oracle Banking, ficantly roducts. of this sult in nsert or f Oracle Banking vell as ess to a EXCUBE cessible ore 6.1 ntegrity Vector: PR:N/UI	NA		A-Ora- Flexc/01- 08- 18/152
Fusion Middlev	vare Mapviewe	r						
NA	18-07-2018	7.5	Vulnerabili Fusion	•	Oracle dleware	NA		A-Ora- Fusio/01-
CV Scoring Scale (CV	/\$\$)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			MapViewer component of Oracle Fusion Middleware (subcomponent: Map Builder). Supported versions that are affected are 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Fusion Middleware MapViewer. Successful attacks of this vulnerability can result in takeover of Oracle Fusion Middleware MapViewer. 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-2018-2943		08- 18/153
	agement Pack				
NA	18-07-2018	4.3	Vulnerability in the Hardware Management Pack component of Oracle Sun Systems Products Suite (subcomponent: Ipmitool). The supported version that is affected is 11.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via IPMI to compromise Hardware Management Pack. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Hardware Management Pack accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:L/I:N/A:N).	NA	A-Ora- Hardw/0 1-08- 18/154

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 Script	ing;								

Vulnerability	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Type(s)			CVE-ID:CVE-2018-2906		
Hospitality Cru	ise Fleet Mana	lement			
NA	18-07-2018	5.5	VulnerabilityintheOracleHospitalityCruiseFleetManagementSystemcomponentofOracleHospitalityApplications(subcomponent:GangwayActivityWebApp)Supportedversionthatisaffectedis9.x.Easilyexploitablevulnerabilityallowslow privilegedattackerwith networkaccess viaHTTPtocompromiseOracleHospitalityCruiseFleetManagementSystem.Successfulattacksofvulnerabilitycanresultunauthorizedcreation,deletion or modificationaccesstocruiseFleetManagementSystemaccessibledataaswellasunauthorizedcreation,deletion or modificationaccesstocruiseFleetManagementSystemaccessibledataasunauthorizedaccessdataor completeaccessManagementSystemaccessibledata.CVSSManagementSystemaccessibledata.CVSSManagementSystemaccessibledata.CVSSManagementSystemaccessibledata.CVSSManagementSystemacc	NA	A-Ora- Hospi/01- 08- 18/155
Hospitality Ope NA	18-07-2018	unuyem 4	Vulnerability in the Oracle	NA	A-Ora-
1421	10 07-2010	T	Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Report Server Config). The supported version that is affected is 5.5.x. Easily	1421	Hospi/01- 08- 18/156

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services 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-2018-3013		
NA	18-07-2018	4	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Reports). The supported version that is affected is 5.5.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services 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-2018-3014	NA	A-Ora- Hospi/01- 08- 18/157

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4.4	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Integration). The supported version that is affected is 5.5.x. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hospitality OPERA 5 Property Services executes to compromise Oracle Hospitality OPERA 5 Property Services. While the vulnerability is in Oracle Hospitality OPERA 5 Property Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality OPERA 5 Property Services. CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI :N/S:C/C:H/I:H/A:H). CVE-ID:CVE-2018-2956	NA	A-Ora- Hospi/01- 08- 18/158
NA	18-07-2018	5	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Integration). The supported version that is affected is 5.5.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can	NA	A-Ora- Hospi/01- 08- 18/159

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			result in unauthorized read access to a subset of Oracle Hospitality OPERA 5 Property Services 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-2018-2955		
NA	18-07-2018	5	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Logging). The supported version that is affected is 5.5.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services 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-2018-2957	NA	A-Ora- Hospi/01- 08- 18/160
Hospitality Sim		-		NY A	
DoS	18-07-2018	6	VulnerabilityintheOracleHospitalitySimphonycomponentofOracleHospitalityApplications(subcomponent:Import/Export).Supportedversionsthat are affected are2.8,2.9and2.10.Difficult toexploitvulnerability	NA	A-Ora- Hospi/01- 08- 18/161

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Simphony accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Simphony accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Simphony. CVSS 3.0 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:H/I:H/A:L). CVE-ID:CVE-2018-2978		
Hyperion Data	Relationship M	lanagen			1
NA	18-07-2018	5	Vulnerability in the Hyperion Data Relationship Management component of Oracle Hyperion (subcomponent: Access and security). The supported version that is affected is 11.1.2.4.330. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Hyperion Data Relationship Management. While the vulnerability is in Hyperion Data Relationship Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	NA	A-Ora- Hyper/01 -08- 18/162

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;									

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID
			unauthorize subset of Relationship accessible d Score 5.8 impacts). (CVSS:3.0/A :N/S:C/C:L/ CVE-ID:CVE Vulnerabilit Financial component (subcompor Models). version tha 11.1.2. Ea vulnerability unauthentic network ac compromise Financial Re vulnerability	d read acce Hyperion Mana ata. CVSS 3 (Confide CVSS V:N/AC:L/F I:N/A:N). -2018-291 ty in the Hy cof Oracle Hy nent: S The sup at is affect asily exp y ated attack cess via H e Hy eporting. W	ess to a Data gement 0 Base entiality Vector: PR:N/UI 5 yperion sporting yperion Security oported cted is loitable allows er with TTP to yperion hile the yperion attacks	Reference/		NCIIPC ID A-Ora- Hyper/01 -08- 18/163
<u>Ilearning</u> NA	18-07-2018	5.8	may sign additional p attacks of th result in un to critical access to Financial Re data. CVSS (Confidentia Vector: (CVSS:3.0/A :N/S:C/C:H/ CVE-ID:CVE	ificantly roducts. Sur- is vulnerabi- nauthorized data or co all H eporting acc 3.0 Base Sc ality impacts V:N/AC:L/F (I:N/A:N). E-2018-290 ty in the	impact ccessful ility can access omplete yperion cessible core 8.6 s). CVSS PR:N/UI 7 Oracle	NA		A-Ora-
	10 07 2010	0.0	iLearning co iLearning Learner Ad supported	omponent o (subcom	f Oracle ponent: n). The			Ilear/01- 08- 18/164
CV Scoring Scale (CV	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iLearning. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iLearning, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iLearning accessible data as well as unauthorized update, insert or delete access to some of Oracle iLearning accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:C/C:H/I:L/A:N). CVE-ID:CVE-2018-2989		
Istore NA	18-07-2018	5	Vulnerability in the Oracle iStore component of Oracle E- Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.0	NA	A-Ora- Istor/01- 08- 18/165

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	-Directory Tr	aversal; DoS-	Denial of Servi	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-2994		
NA	18-07-2018	5.8	Vulnerability in the Oracle iStore component of Oracle E- Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity 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-2018-2995	NA	A-Ora- Istor/01- 08- 18/166
NA	18-07-2018	5.8	Vulnerability in the Oracle iStore component of Oracle E- Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2,	NA	A-Ora- Istor/01- 08- 18/167

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 Script	Sql-SQL Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity 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-2018-3018		
	terpriseone Too				
NA	18-07-2018	4	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	NA	A-Ora- Jd/01-08- 18/168

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Servi	ce; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			JD Edwards EnterpriseOne Tools 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-2018-2947		
NA	18-07-2018	5	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Monitoring and Diagnostics). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools 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-2018-2944	NA	A-Ora- Jd/01-08- 18/169
NA	18-07-2018	5.8	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require	NA	A-Ora- Jd/01-08- 18/170

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	5.8	human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools 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-2018-2945 Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD	NA	A-Ora- Jd/01-08- 18/171

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools 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-2018-2946		
NA	18-07-2018	5.8	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools 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).	NA	A-Ora- Jd/01-08- 18/172

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;										

Vulnerability Type(s)	Publish Date	CVSS	Descri	otion & CVE	ID	Reference	/Patch	NCIIPC ID
JF - (-)			CVE-ID:CVE	2-2018-294	8			
NA	18-07-2018	5.8	Vulnerabil Edwards En component Edwards (subcompon Runtime). version tha Easily explo- allows attacker wi via HTTP Edwards En Successful human int person othe and while fi in JD Edwa Tools, attach impact ad Successful vulnerabilit unauthorized delete acce Edwards En accessible unauthorized subset o Enterprise data. CVSS	ity in the nterpriseOn of Orac Paent: The sup t is affected bitable vulnes unauthen th network to compror attacks teraction f er than the a the vulneral ords Enterp ks may signi ditional pr attacks of y can res ed update, in ss to some nterpriseOn data as w ed read acce f JD E one Tools ac 3.0 Base Sc ality and In CVSS W:N/AC:L/H I:L/A:N).	he JD e Tools cle JD roducts Web oported l is 9.2. erability nticated access nise JD e Tools. require rom a attacker bility is riseOne ficantly roducts. of this sult in nsert or e of JD e Tools vell as ess to a dwards cessible core 6.1 ntegrity Vector: PR:N/UI	NA		A-Ora- Jd/01-08- 18/173
NA	18-07-2018	5.8	Vulnerabil Edwards En component Edwards (subcompon Runtime). version tha Easily explo	A-Ora- Jd/01-08- 18/174				
		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
	10.07.2010		attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools 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-2018-2950		
NA	18-07-2018	5.8	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products.	NA	A-Ora- Jd/01-08- 18/175

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Servi	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools 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-2018-2999		
NA	18-07-2018	5.8	CVE-DFCVE-2010-2999 Vulnerability in the JDEdwards EnterpriseOne Toolscomponent of Oracle JDEdwards Products(subcomponent: WebRuntime). The supportedversion that is affected is 9.2.Easily exploitable vulnerabilityallows unauthenticatedattacker with network accessvia HTTP to compromise JDEdwards EnterpriseOne Tools.Successful attacks requirehuman interaction from aperson other than the attackerand while the vulnerability isin JD Edwards EnterpriseOneTools, attacks may significantlyimpact additional products.Successful attacks of thisvulnerability can result inunauthorized update, insert ordelete access to some of JDEdwards EnterpriseOne Toolsaccessible data as well asunauthorized read access to asubset of JD EdwardsEnterpriseOne Tools accessibledata. CVSS 3.0 Base Score 6.1	NA	A-Ora- Jd/01-08- 18/176

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;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-3006		
JDK,JRE					
NA	18-07-2018	4.3	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). The supported version that is affected is Java SE: 10.0.1. 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 access to critical data or complete access to all Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:H/I:N/A:N). CVE-ID:CVE-2018-2972	https://security.n etapp.com/adviso ry/ntap- 20180726-0001/	A-Ora- JDK,J/01- 08- 18/178
NA	18-07-2018	4.3	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JSSE). Supported versions that are	https://security.n etapp.com/adviso ry/ntap- 20180726-0001/,	A-Ora- JDK,J/01- 08- 18/179

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, 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 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:N/I:H/A:N). CVE-ID:CVE-2018-2973	https://access.red hat.com/errata/R HSA-2018:2253, https://access.red hat.com/errata/R HSA-2018:2254, https://access.red hat.com/errata/R HSA-2018:2255, https://access.red hat.com/errata/R HSA-2018:2256	
NA	18-07-2018	4.3	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Easily exploitable vulnerability allows unauthenticated	https://access.red hat.com/errata/R HSA-2018:2255, https://access.red hat.com/errata/R HSA-2018:2256, https://security.n etapp.com/adviso	A-Ora- JDK,J/01- 08- 18/180

	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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. 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 Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, 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 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:U/C:L/I:N/A:N). CVE-ID:CVE-2018-2940	ry/ntap- 20180726-0001/, https://access.red hat.com/errata/R HSA-2018:2254, https://access.red hat.com/errata/R HSA-2018:2253	
NA	18-07-2018	5.1	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u172 and 10.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a	https://access.red hat.com/errata/R HSA-2018:2256, https://access.red hat.com/errata/R HSA-2018:2253, https://security.n etapp.com/adviso ry/ntap- 20180726-0001/	A-Ora- JDK,J/01- 08- 18/181

CV Scoring Scale (CVSS)	3-4	4-5	5-0	0-7	/-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;										

Vulnerability Type(s)	Publish Date	CVSS	Descrip	tion & CVE	ID	Reference	Patch	NCIIPC ID
			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, 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 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:R/S:C/C:H/I:H/A:H). CVE-ID:CVE-2018-2964					
NA	18-07-2018	5.1					rata/R 256, ess.red rata/R 253, urity.n adviso 0001/, ess.red rata/R	A-Ora- JDK,J/01- 08- 18/182
CV Scoring Scale (C Vulnerability Type(-	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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, 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 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:R/S:C/C:H/I:H/A:H). CVE-ID:CVE-2018-2941	https://access.red hat.com/errata/R HSA-2018:2254	
NA	18-07-2018	5.1	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Windows DLL). Supported versions that are affected are Java SE: 7u181 and 8u172. 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: Applies to client and server	https://security.n etapp.com/adviso ry/ntap- 20180726-0001/	A-Ora- JDK,J/01- 08- 18/183

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:R/S:C/C:H/I:H/A:H). CVE-ID:CVE-2018-2942		
NA	18-07-2018	6.8	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Java DB). Supported versions that are affected are Java SE: 6u191, 7u181 and 8u172. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. 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 can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVE-2018-2938 addresses CVE-2018-1313. CVSS 3.0 Base Score 9.0	https://security.n etapp.com/adviso ry/ntap- 20180726-0001/	A-Ora- JDK,J/01- 08- 18/184

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:C/C:H/I:H/A:H). CVE-ID:CVE-2018-2938		
JDK,JRE,Jrockit		4.2	Vulnershility in the lave CE	https://acqurity.p	A 0m
DoS	18-07-2018	4.3	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. Difficult to exploit 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: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:N/I:N/A:L).	https://security.n etapp.com/adviso ry/ntap- 20180726-0001/, https://access.red hat.com/errata/R HSA-2018:2254, https://access.red hat.com/errata/R HSA-2018:2255, https://access.red hat.com/errata/R HSA-2018:2256, https://access.red hat.com/errata/R HSA-2018:2241, https://access.red hat.com/errata/R HSA-2018:2253, https://access.red hat.com/errata/R HSA-2018:2253, https://access.red hat.com/errata/R HSA-2018:2242	A-Ora- JDK,J/01- 08- 18/177

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2952		
Marketing					
NA	18-07-2018	4	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Products). 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. Difficult to exploit 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 6.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:R/S:C/C:H/I:L/A:N). CVE-ID:CVE-2018-2988	NA	A-Ora- Marke/01 -08- 18/185
NA	18-07-2018	5.8	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated	NA	A-Ora- Marke/01 -08- 18/186

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			attacker with network access via HTTP to compromise 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-2018-3008		
Micros Relate (Customer Relati	ionship	Management Software	I	
DoS	18-07-2018	5.5	Vulnerability in the MICROS Relate CRM Software component of Oracle Retail Applications (subcomponent: Internal Operations). Supported versions that are affected are 10.8.x and 11.4.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Relate CRM Software. While the vulnerability is in MICROS Relate CRM Software, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some	NA	A-Ora- Micro/01- 08- 18/187

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 Script	ing;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			of MICROS Relate CRM Software accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MICROS Relate CRM Software. CVSS 3.0 Base Score 6.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:C/C:N/I:L/A:L). CVE-ID:CVE-2018-3052		
Micros Retail-j					
DoS	18-07-2018	3.7	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Back Office). Supported versions that are affected are 10.2.x, 11.0.x, 12.0.x, 12.1.x, 12.1.1.x,12.1.2.x and 13.1.x. Difficult to exploit vulnerability allows physical access to compromise MICROS Retail-J. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MICROS Retail-J, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MICROS Retail-J accessible data as well as unauthorized access to critical data or complete access to all MICROS Retail-J accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MICROS Retail-J. CVSS 3.0 Base Score	NA	A-Ora- Micro/01- 08- 18/188

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:P/AC:H/PR:H/U I:R/S:C/C:H/I:H/A:L). CVE-ID:CVE-2018-2888 		
DoS	18-07-2018	6.5	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Database). Supported versions that are affected are 11.0.x, 12.0.x, 12.1.x, 12.1.1.x, 12.1.2.x and 13.1.x. Easily exploitable vulnerability allows low privileged 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 and unauthorized ability to cause a partial denial of service (partial DOS) of MICROS Retail-J. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:L). CVE-ID:CVE-2018-2881	NA	A-Ora- Micro/01- 08- 18/189
NA	18-07-2018	4	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Interfaces). Supported versions that are affected are 10.2.x, 11.0.x, 12.0.x,12.1.x, 12.1.1.x,12.1.2.x and 13.1.x. Easily exploitable	NA	A-Ora- Micro/01- 08- 18/190

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 Script	ing;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Retail-J. While the vulnerability is in MICROS Retail-J, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MICROS Retail-J accessible data. CVSS 3.0 Base Score 7.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:C/C:N/I:H/A:N). CVE-ID:CVE-2018-2882		
Mysql NA	18-07-2018	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via memcached 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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:N/I:N/A:H). CVE-ID:CVE-2018-3062	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/191
NA	18-07-2018	3.5	Vulnerability in the MySQL Server component of Oracle		A-Ora- Mysql/01

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(c), CSDE (rocc Site Dequest Forgery, Dir, Tray, Directory Trayersal, DeS, Depial of Service, NA, Net Applica								

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:L/I:N/A:N). CVE-ID:CVE-2018-2767	ry/ntap- 20180726-0002/	-08- 18/192
NA	18-07-2018	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.11 and prior. Difficult to exploit 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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :N/S:U/C:N/I:N/A:H). CVE-ID:CVE-2018-3074	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/193

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	7Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Audit Log). Supported versions that are affected are 5.7.22 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-2018-3071	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/194
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 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-2018-3070	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/195

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.11 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-2018-3079	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/196
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: MyISAM). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 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-2018-3058	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/197

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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-2018-3054	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/198
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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-2018-3077	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/199

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 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-2018-3078	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/200
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 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-2018-3080	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/201

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;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018 4		Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 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 read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI :N/S:U/C:L/I:N/A:N). CVE-ID:CVE-2018-3082	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/202
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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-2018-3065	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/203

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	7Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 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-2018-3061	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/204
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.11 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-2018-3073	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/205

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;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA			Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.11 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-2018-3067	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/206
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.60 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-2018-3063	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/207

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.22 and prior and 8.0.11 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 read access to a subset of MySQL 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-2018-3056	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/208
NA	18-07-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.11 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-2018-3075	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/209

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4.9	Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/U I:N/S:U/C:N/I:L/A:H). CVE-ID:CVE-2018-3081	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/210
NA	18-07-2018	4.9	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 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 update, insert or delete access to some of MySQL Server accessible	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/211

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID	
			data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/U I:N/S:U/C:L/I:L/A:N). CVE-ID:CVE-2018-3066			
NA	18-07-2018	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:H). CVE-ID:CVE-2018-3064	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/212	
NA	18-07-2018	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/213	

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI :N/S:U/C:N/I:H/A:H). CVE-ID:CVE-2018-3060		
Mysql Workbe	nch		CVE-ID:CVE-2010-3000		
NA NA	18-07-2018	4.3	Vulnerability in the MySQL Workbench component of Oracle MySQL (subcomponent: Workbench: Security: Encryption). Supported versions that are affected are 6.3.10 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Workbench. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Workbench accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:L/I:N/A:N). CVE-ID:CVE-2018-2598	https://security.n etapp.com/adviso ry/ntap- 20180726-0002/	A-Ora- Mysql/01 -08- 18/214

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA Order Manage	18-07-2018	5.8	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E- Business Suite (subcomponent: Print Server). 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 One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, 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 One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment 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-2018-2953	NA	A-Ora- One-t/01- 08- 18/215
NA	18-07-2018	4.4	Vulnerability in the Oracle Order Management component of Oracle E-Business Suite (subcomponent: Product Diagnostic Tools). Supported versions that are affected are	NA	A-Ora- Order/01 -08- 18/216

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Order Management executes to compromise Oracle Order Management. Successful attacks of this vulnerability can result in takeover of Oracle Order Management. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI :N/S:U/C:H/I:H/A:H). CVE-ID:CVE-2018-2954		
Outside In Tech					
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-Ora- Outsi/01- 08- 18/217

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-2992		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-Ora- Outsi/01- 08- 18/218

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3009		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-Ora- Outsi/01- 08- 18/219

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3010		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-0ra- Outsi/01- 08- 18/220

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3092		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-0ra- Outsi/01- 08- 18/221

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3093		
DoS	18-07-2018	5.8	VulnerabilityintheOracleOutsideInTechnologycomponentofOracleFusionMiddleware(subcomponent:OutsideInFilters).Thesupportedversionthatisaffectedis8.5.3.EasilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromiseOracleOutsideInTechnology.Successfulattacksrequirehumaninteractionfrom aperson otherthan the attacker.Successfulattacksofunauthorizedaccesstounauthorizedaccesstodataorcompleteaccessibledataandunauthorizedabilitytoauataapartialdenialofservice(partial DOS)ofOracleOutsideInTechnology.	NA	A-Ora- Outsi/01- 08- 18/222

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3094		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-0ra- Outsi/01- 08- 18/223

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

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 this08- 18/224	Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
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		18-07-2018	5.8	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-2018-3095 Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service	NA	Outsi/01- 08-

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3096		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-Ora- Outsi/01- 08- 18/225

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3097		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-Ora- Outsi/01- 08- 18/226

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3098		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-0ra- Outsi/01- 08- 18/227

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3099		
DoS	18-07-2018	5.8	CVE-DECVE-2018-3099Vulnerability in the OracleOutsideInTechnologycomponent of Oracle FusionMiddleware(subcomponent:OutsideInFilters).Thesupportedversion that isaffectedis8.5.3.Easilyexploitablevulnerabilityallowsunauthenticatedattacker with network accessviaHTTPtocompromiseOracleOutsideInTechnology.Successfulattacksvequirehumaninteractionfrom aperson other than the attacker.Successfulattacksvulnerabilitycanresultinunauthorizedaccess todataorcompleteaccess toaccessibledatadataandunauthorizedability to cause apartialdenialofservice(partial DOS) of Oracle OutsideInTechnology.	NA	A-Ora- Outsi/01- 08- 18/228

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3102		
DoS	18-07-2018	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	A-Ora- Outsi/01- 08- 18/229

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3103		
DoS	18-07-2018	5.8	CVE-DECVE-2018-ST03Vulnerability in the OracleOutsideInTechnologycomponent of Oracle FusionMiddleware(subcomponent:OutsideInFilters).Thesupportedversion that isaffectedis8.5.3.Easilyexploitablevulnerabilityallowsunauthenticatedattacker with network accessviaHTTPtocompromiseOracleOutsideInTechnology.Successfulattacksrequirehumaninteractionperson other than the attacker.Successfulattacksvulnerabilitycanresultinunauthorizedaccess todataorormpleteaccess toaccessibledatadataandunauthorizedability to cause apartialdenialofservice(partial DOS) of Oracle OutsideInTechnology.	NA	A-Ora- Outsi/01- 08- 18/230

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3104		
	erprise Cs Finar				
NA	18-07-2018	4	Vulnerability in the PeopleSoft Enterprise CS Financial Aid component of Oracle PeopleSoft Products (subcomponent: ISIR Processing). Supported versions that are affected are 9.0 and 9.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Financial Aid. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Financial Aid accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI :N/S:U/C:L/I:N/A:N). CVE-ID:CVE-2018-3076	NA	A-Ora- Peopl/01- 08- 18/231

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;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Peoplesoft Ente	erprise Human	Capital	Management Human Resources		
NA	18-07-2018	5.8	Vulnerability in the PeopleSoft Enterprise HCM Human Resources component of Oracle PeopleSoft Products (subcomponent: Compensation). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Human Resources, 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 HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources 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-2018-3068	NA	A-Ora- Peopl/01- 08- 18/232
Peoplesoft Ente	•		Vulnovability in the	NA	A 0ro
NA	18-07-2018	4	VulnerabilityinthePeopleSoftEnterprisePeopleToolscomponentOraclePeopleSoftProducts(subcomponent:PIASearchFunctionality).Supported	NA	A-Ora- Peopl/01- 08- 18/233

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows low privileged 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 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-2018-2970		
NA	18-07-2018	4.3	VulnerabilityinthePeopleSoftEnterprisePeopleToolscomponentOraclePeopleSoftProducts(subcomponent:IntegrationBroker).Supportedversionsthat are affected are 8.55 and8.56.Easilyexploitablevulnerabilityallowsunauthenticatedattacker withnetworkaccessviaHTTPtocompromisePeopleSoftEnterprisePeopleTools.Successfulattacksrequirehumaninteractionfrom aperson other than the attacker.Successfulattacksofsuccessfulattacksofunauthorizedaccesstounauthorized accesstoattacker.SuccessfulattacksofunauthorizedaccesstopeopleSoftEnterprisePeopleSoftEnterprisePeopleToolsaccessibledataorcompleteaccessPeopleToolsaccessibledata.CVSSCVSS3.0BaseScoreGonfidentialityimpacts).CVSSVector:(CVSS:3.0/AV:N/AC:L/PR:N/UI	NA	A-Ora- Peopl/01- 08- 18/234

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 Script	ing;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			:R/S:U/C:H/I:N/A:N). CVE-ID:CVE-2018-2977		
NA	18-07-2018	5.5	VulnerabilityinthePeopleSoftEnterprisePeopleToolscomponentOraclePeopleSoftProducts(subcomponent:IntegrationBroker).Supportedversionsthat are affected are8.55and8.56.EasilyexploitablevulnerabilityallowslowprivilegedattackerwithnetworkaccessviaSuccessfulattacksofSuccessfulattacksofvulnerabilitycanresultinunauthorizedupdate, insert ordeleteaccesstoPeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleToolsaccessibledataaswellasunauthorizedreadaccesstoasubsetofPeopleSoftPeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnte	NA	A-Ora- Peopl/01- 08- 18/235
NA	18-07-2018	5.8	VulnerabilityinthePeopleSoftEnterprisePeopleToolscomponentOraclePeopleSoftProducts(subcomponent:IntegrationBroker).Supportedversionsthat are affected are8.55 and8.56.DifficulttoexploitvulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromisePeopleSoftEnterprise	NA	A-Ora- Peopl/01- 08- 18/236

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;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:H/I:H/A:N). CVE-ID:CVE-2018-2990		
NA	18-07-2018	5.8	VulnerabilityinthePeopleSoftEnterprisePeopleToolscomponentOraclePeopleSoftProducts(subcomponent:PIACoreTechnology).Supportedversionsthat are affected are8.55and8.56.Easilyexploitablevulnerabilityallowsunauthenticatedattackerwith network accessviaHTTPtoPeopleSoftEnterprisePeopleTools.Successfulattacksrequirehumaninteractionfrom a personotherthan the attacker andwhilethe vulnerability is inPeopleSoftEnterprisePeopleTools,attacksmuthersignificantly impact additionalproducts.Successful attacks ofthis vulnerability can result inunauthorized update, insert ordeleteaccesstosome ofPeopleSoftEnterprise	NA	A-Ora- Peopl/01- 08- 18/237

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Servi	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-2929		
NA	18-07-2018	5.8	VulnerabilityinthePeopleSoftEnterprisePeopleToolscomponentOraclePeopleSoftProducts(subcomponent:UnifiedNavigation).Supportedversionsthat are affected are8.55and8.56.Easilyexploitablevulnerabilityallowsunauthenticatedattacker with network accessviaHTTPtoPeopleSoftEnterprisePeopleTools.Successfulattacksrequirehumaninteractionfrom a personother than the attacker andwhile the vulnerability is inPeopleSoftEnterprisePeopleTools,attacksattacksrequirenuauthorized update, insertproducts.Successful attacks ofthis vulnerability can result inunauthorized update, insert ordeleteaccessPeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprise <t< td=""><td>NA</td><td>A-Ora- Peopl/01- 08- 18/238</td></t<>	NA	A-Ora- Peopl/01- 08- 18/238

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;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-2919		
NA	18-07-2018	5.8	VulnerabilityinthePeopleSoftEnterprisePeopleToolscomponentOraclePeopleSoftProducts(subcomponent:Workflow).Supportedversionsthataffectedare8.55and8.55and8.56.Easilyexploitablevulnerabilityallowsunauthenticatedattackerwith networkaccessviaHTTPtocompromisePeopleSoftEnterprisePeopleTools.SuccessfulattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleTools,attacksmaysignificantlyimpactadditionalproducts.Successfulattacks ofthisvulnerabilitycan resultinunauthorizedupdate,insert ordeleteaccesstosomePeopleSoftEnterprisePeopleSoftPeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprisePeopleSoftEnterprise	NA	A-Ora- Peopl/01- 08- 18/239
NA	18-07-2018	5.8	VulnerabilityinthePeopleSoftEnterprisePeopleToolscomponentofOraclePeopleSoftProducts(subcomponent:Workflow).	NA	A-Ora- Peopl/01- 08- 18/240

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Servi	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-2986		
Peoplesoft Hun					
NA	18-07-2018	5	Vulnerability in the PeopleSoft HRMS component of Oracle PeopleSoft Products (subcomponent: Candidate Gateway). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft HRMS. Successful attacks of this vulnerability can	NA	A-Ora- Peopl/01- 08- 18/241

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			result in unauthorized read access to a subset of PeopleSoft HRMS 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-2018-3072		
	· · · · · · · · · · · · · · · · · · ·	-	folio Management	NA	A Ore
NA	18-07-2018	3.6	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.x, 16.x and 17.x. Difficult to exploit vulnerability allows low privileged 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 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.	NA	A-Ora- Prima/01 -08- 18/242

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVSS 3.0 Base Score 4.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI :R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-2962		
NA	18-07-2018	4	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.x and 16.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management 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-2018-2963	NA	A-Ora- Prima/01 -08- 18/243
NA	18-07-2018	5.8	VulnerabilityinthePrimaveraP6EnterpriseProjectPortfolioMaragementcomponentofOracleConstructionandEngineeringSuite(subcomponent:WebAccess).Supportedversionsthat are affected are8.4, 15.x,16.xand17.x.Easilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetwork	NA	A-Ora- Prima/01 -08- 18/244

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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 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-2018-2960		
NA	18-07-2018	5.8	VulnerabilityinthePrimaveraP6EnterpriseProject PortfolioManagementcomponentofOracleConstructionand EngineeringSuite(subcomponent:WebAccess).Supportedversionsthat are affected are8.4, 15.x,16.xand17.x.Easilyexploitablevulnerabilityallowsunauthenticatedattacker withnetworkaccessviaHTTPtocompromisePrimaveraP6EnterpriseProject PortfolioManagement.Successfulattacksrequire	NA	A-Ora- Prima/01 -08- 18/245

	8-9	7-8	8-9	9-10				
Sqr SQL injection, ASS Gross Site Seripting,	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)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-2961		
Primavera Uni NA	<u>fier</u> 18-07-2018	4	VulnerabilityinthePrimaveraUnifiercomponentofOracleConstructionandEngineeringSuite(subcomponent:Core).Thesupportedversionthatisaffectedis16.x.EasilyexploitablevulnerabilityallowslowprivilegedattackerwithnetworkaccessviaHTTPtocompromisePrimaveraUnifier.SuccessfulattacksofthisvulnerabilitycanresultinunauthorizedreadaccesstoasubsetofPrimaveraUnifieraccessibleaccessibledata.CVSS3.0BaseScore4.3(Confidentialityimpacts).CVSS(CVSS:3.0/AV:N/AC:L/PR:L/UI	NA	A-Ora- Prima/01 -08- 18/246

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 Script	Sql-SQL Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			:N/S:U/C:L/I:N/A:N). CVE-ID:CVE-2018-2969		
NA	18-07-2018	4.3	VulnerabilityinthePrimaveraUnifiercomponentofOracleConstructionandEngineeringSuite(subcomponent:Core).Supportedversionsthatareaffected are16.x, 17.xaffectedare16.x, 17.xallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromisePrimaveraUnifier.Successfulattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfrom <tr< td=""><td>NA</td><td>A-Ora- Prima/01 -08- 18/247</td></tr<>	NA	A-Ora- Prima/01 -08- 18/247
NA	18-07-2018	4.3	VulnerabilityinthePrimaveraUnifiercomponentofOracleConstructionandEngineeringSuite(subcomponent:Core).Supportedversionsthat areaffected are16.x, 17.x and18.x.EasilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetworkviaHTTPtocompromisePrimaveraUnifier.Successfulattacksrequirehuman	NA	A-Ora- Prima/01 -08- 18/248

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;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Primavera Unifier accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:U/C:N/I:H/A:N). CVE-ID:CVE-2018-2968		
NA	18-07-2018	5.8	VulnerabilityinthePrimaveraUnifiercomponentofOracleConstructionandEngineeringSuite(subcomponent:Core).Thesupportedversionthatisaffectedis16.x.EasilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetworkattackerwithnetworkPrimaveraUnifier.SuccessfulattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapersonotherthanotherthantheattacksrequirehumaninteractionfromapersonotherthanthevulnerabilityisinprimaveraUnifier, attacksproducts.SuccessfulattacksprimaveraUnifieraccessibledataaswellasdataasunauthorizedreadaccesstoasubsetofPrimaveraUnifieraccessibledata.CVSSVector:(Conf	NA	A-Ora- Prima/01 -08- 18/249

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Type(s)		CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2965		
Retail Bulk Da	ta Integration				
NA	18-07-2018	5.8	Vulnerability in the Oracle Retail Bulk Data Integration component of Oracle Retail Applications (subcomponent: BDI Job Scheduler). The supported version that is affected is 16.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Bulk Data Integration. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Retail Bulk Data Integration, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Bulk Data Integration accessible data as well as unauthorized read access to a subset of Oracle Retail Bulk Data Integration 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-2018-2891	NA	A-Ora- Retai/01- 08- 18/250
			mentation Foundation		
DoS	18-07-2018	5.5	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation component of Oracle Retail Applications (subcomponent: Internal Operations).	NA	A-Ora- Retai/01- 08- 18/251

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Supported versions that are affected are 16.x and 17.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. While the vulnerability is in Oracle Retail Customer Management and Segmentation Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Customer Management and Segmentation Foundation accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Customer Management and Segmentation Foundation. CVSS 3.0 Base Score 6.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:C/C:N/I:L/A:L). CVE-ID:CVE-2018-3053		
Scripting					
NA	18-07-2018	5.8	Vulnerability in the Oracle Scripting component of Oracle E-Business Suite (subcomponent: Script Author). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise	NA	A-Ora- Scrip/01- 08- 18/252

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		ery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, 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 Scripting accessible data as well as unauthorized update, insert or delete access to some of Oracle Scripting 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-2018-2997		
Siebel Ui Frame	ework				
NA	18-07-2018	4.3	Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). The supported version that is affected is 18.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS	NA	A-Ora- Siebe/01- 08- 18/253

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:U/C:N/I:L/A:N). CVE-ID:CVE-2018-2959		
Soa Suite					
NA	18-07-2018	4	Vulnerability in the Oracle SOA Suite component of Oracle Fusion Middleware (subcomponent: Health Care FastPath). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle SOA Suite 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-2018-3105	NA	A-Ora- Soa/01- 08- 18/254
Solaris Cluster					
NA	18-07-2018	7.5	Vulnerability in the Solaris Cluster component of Oracle Sun Systems Products Suite (subcomponent: NAS device addition). Supported versions that are affected are 3.3 and 4.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via RPC to compromise Solaris Cluster. Successful attacks of this vulnerability can result in takeover of Solaris Cluster. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and	NA	A-Ora- Solar/01- 08- 18/255

CV Scoring Scale (CVSS)	3-4	4-5	5-0	6-7	/-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 Script	ing;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-2930		
Trade Manage	ment				
NA	18-07-2018	5.8	Vulnerability in the Oracle TradeManagement Managementcomponent of Oracle E- BusinessSuite(subcomponent:UserInterface). 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 exploitablevulnerability allowsunauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is 	NA	A-Ora- Trade/01 -08- 18/256
NA	18-07-2018	5.8	Vulnerability in the OracleTradeManagement	NA	A-Ora- Trade/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. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable;								

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			component of Oracle E- Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:C/C:H/I:L/A:N). CVE-ID:CVE-2018-3012		-08- 18/257
Tuxedo NA	18-07-2018	5	Vulnerability in the OracleTuxedo component of OracleFusionMiddleware(subcomponent:Core).Supported versions that areaffected are 12.1.1, 12.1.3 and12.2.2.Easilyexploitablevulnerabilityallowsunauthenticated attacker with	NA	A-Ora- Tuxed/01 -08- 18/258

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			network access via Jolt to compromise Oracle Tuxedo. While the vulnerability is in Oracle Tuxedo, 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 Tuxedo accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :N/S:C/C:H/I:N/A:N). CVE-ID:CVE-2018-3007		
Vm Virtualbox		2.2	Wala anakilita in the Oreale VM	NI A	A 0mg
NA	18-07-2018	3.3	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. 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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox	NA	A-Ora- Vm/01- 08- 18/259

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI :R/S:C/C:L/I:N/A:H). CVE-ID:CVE-2018-3055		
NA	18-07-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. 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-2018-3086	NA	A-Ora- Vm/01- 08- 18/260
NA	18-07-2018	4.4	Vulnerability in the Oracle VMVirtualBoxcomponentOracleVirtualization(subcomponent:Core).ThesupportedversionthataffectedisPriorto5.2.16.Easilyexploitablevulnerabilityallowsunauthenticated	NA	A-Ora- Vm/01- 08- 18/261

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	4.4	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-2018-3087 Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in 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	NA	A-Ora- Vm/01- 08- 18/262

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3088		
NA	18-07-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. 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-2018-3089	NA	A-Ora- Vm/01- 08- 18/263
NA	18-07-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated attacker with logon to the	NA	A-Ora- Vm/01- 08- 18/264

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3090		
NA	18-07-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. 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 unauthorized creation, deletion or modification access to critical data or all Oracle VM	NA	A-Ora- Vm/01- 08- 18/265

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 Script	ing;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI :R/S:C/C:L/I:H/A:H). CVE-ID:CVE-2018-3085		
Webcenter Por					
NA	18-07-2018	5	Vulnerability in the Oracle WebCenter Portal component of Oracle Fusion Middleware (subcomponent: Portlet Services). Supported versions that are affected are 11.1.1.9.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Portal accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :N/S:U/C:L/I:N/A:N). CVE-ID:CVE-2018-3101	NA	A-Ora- Webce/0 1-08- 18/266
Weblogic Serve					
DoS	18-07-2018	5.8	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: JSF). Supported versions that are affected are 10.3.6.0, 12.1.3.0,	NA	A-Ora- Weblo/01 -08- 18/267

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			12.2.1.2 and 12.2.1.3. 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 attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic 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-2018-2935		
NA	18-07-2018	5.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: SAML). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. 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 update, insert or delete access to some	NA	A-Ora- Weblo/01 -08- 18/268

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	/Directory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N). CVE-ID:CVE-2018-2998		
NA	18-07-2018	5.8	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Console). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. 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).	NA	A-Ora- Weblo/01 -08- 18/269

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2987		
NA	18-07-2018	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, 12.2.1.2 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-2018-2893	NA	A-Ora- Weblo/01 -08- 18/270
NA	18-07-2018	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 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 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).	NA	A-Ora- Weblo/01 -08- 18/271

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 Script	ing;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2894		
Orderbook Pre	esale Token Pro	oject			
Orderbook Pre	sale Token				
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Orderbook Presale Token (OBP), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13676	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Pres aleToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Ord- Order/01 -08- 18/272
Otakutoken Pr	oject				
Otakutoken				1	
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for OTAKUToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13755	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/OTA KUToken	A-Ota- Otaku/01 -08- 18/273
Pelocointoken	Project				
Pelocointoken				1	
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for PELOCoinToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13738	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/PEL OCoinToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2	A-Pel- Peloc/01- 08- 18/274
		3-4	4-5 5-6 6-7	7-8 8-9	9-10

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	EID	Reference/	Patch	NCIIPC ID
						0integer%20 low.md	Ooverf	
Play2liveprom	o Project							
Play2liveprom								
Overflow	09-07-2018	5	smart contra	2LivePromo oken, has an at allows the ntract to a n arbitrary	entation o, an integer e owner set the user to	https://gith m/BlockCha urity/Ether /tree/maste 2LivePromo https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md	insSec Fokens r/Play , ub.co insSec Fokens er/GE int%2	A-Pla- Play2/01- 08- 18/275
Pmet Project								
Pmet	1							
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for PMET, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13712			https://gith m/BlockCha urity/Ether /tree/maste ET, https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md	insSec Fokens r/PM ub.co insSec Fokens er/GE int%2	A-Pme- Pmet/01- 08- 18/276
Pmhtoken Pro	ject							
Pmhtoken Overflow	09-07-2018	5	smart contract implementationmfor PMHToken, an Ethereumutoken, has an integer overflow/4that allows the owner of theHcontract to set the balance ofan arbitrary user to any value. CVE-ID:CVE-2018-13705 muu			https://gith m/BlockCha urity/Ether /tree/maste HToken, https://gith m/BlockCha urity/Ether /blob/maste	insSec Fokens pr/PM ub.co insSec Fokens	A-Pmh- Pmhto/0 1-08- 18/277
CV Scoring Scale (C		3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s):CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;
Sql-SQL Injection; XSS- Cross Site Scripting;

Type(s) Type(s) Projectj Project Projectj Overflow Image: state states	09-07-2018	5	smart contr for Projec token, has a	oken functio act impleme tJ, an Etl	ntation	MCHAIN/mi Ointeger%20 low.md https://gith m/BlockCha	0overf ub.co	A-Pro-
Projectj Overflow		5	smart contr for Projec token, has a	act impleme	ntation			-
Overflow	09-07-2018	5	smart contr for Projec token, has a	act impleme	ntation			-
Rckt Coin Proiec			contract to an arbitrary	the owner set the ball user to any 2-2018-137	of the ance of y value.	urity/Ether7 /tree/maste ectJ, https://gith m/BlockCha urity/Ether7 /blob/maste MCHAIN/mi 0integer%20 low.md	Fokens er/Proj ub.co ainsSec Fokens er/GE int%2	Proje/01- 08- 18/278
	ct					10 w.111u		
Rckt Coin								
	09-07-2018	5	smart contr for RCKT_C token, has a that allows contract to an arbitrary	an integer o	ntation hereum verflow of the ance of y value.	https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md,	ainsSec Fokens er/GE int%2	A-Rck- Rckt/01- 08- 18/279
						https://gith m/BlockCha urity/Ether /tree/maste T_Coin	ainsSec Tokens	
Redticket Projec	ct							
Redticket								
Overflow	09-07-2018	5	smart contr for RedTic token, has a that allows contract to	an integer of the owner set the bal vuser to any	ntation hereum verflow of the ance of	https://gith m/BlockCha urity/Ether /tree/maste Ticket, https://gith	ainsSec Fokens er/Red	A-Red- Redti/01- 08- 18/280
				-2010-120	96	m/BlockCha		

CV Scoring Scale (CVSS)3-44-55-66-77-88-99-10Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable;

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				/blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
Richiumtoken	Project				
Richiumtoken Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for RichiumToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13750	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Rich iumToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Ric- Richi/01- 08- 18/281
Riptidecoin Pro	oject				
Riptidecoin Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for RiptideCoin (RIPT), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13732	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Ript ideCoin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Rip- Ripti/01- 08- 18/282
Robotbtc Proje	ect				
Robotbtc					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for RobotBTC, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13697	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Rob otBTC, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Rob- Robot/01 -08- 18/283
Rocket Coin Pr	oject				
Rocket Coin					
Overflow	12-07-2018	5	An integer overflow vulnerability exists in the function multiTransfer of Rocket Coin (XRC), an Ethereum token smart contract. An attacker could use it to set any user's balance. CVE-ID:CVE-2018-13836	https://github.co m/VenusADLab/E therTokens/tree/ master/Rocket%2 0Coin%28XRC%2 9, https://github.co m/VenusADLab/E therTokens/blob/ master/SHARKTE CH/SHARKTECH. md	A-Roc- Rocke/01 -08- 18/284
Rrtoken Proje	ct			ind	
Rrtoken					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for RRToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13777	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co	A-Rrt- Rrtok/01- 08- 18/285
Rtokenmain P CV Scoring Scale (C	vss)	3-4	4-5 5-6 6-7 Forgery; Dir. TravDirectory Traversal; Do	m/BlockChainsSec urity/EtherTokens /tree/master/RRT oken 7-8 8-9	9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	EID	Reference/	'Patch	NCIIPC ID
Rtokenmain								
Overflow	09-07-2018	5	The mintT smart contra for R Time (Contract Na an Ethereu integer ove the owner o the balance user to any CVE-ID:CVE	e Token v ame: RToke m token, erflow that f the contra e of an a value.	entation v3 (RS) nMain), has an allows ct to set rbitrary 91	https://gith m/BlockCha urity/Ether /tree/maste kenMain, https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md	insSec Fokens r/RTo ub.co insSec Fokens er/GE int%2	A-Rto- Rtoke/01 -08- 18/286
Servviziotoken	Project							
<u>Servviziotoken</u> Overflow	09-07-2018	5	smart contra	VIZIOToken oken, has an at allows the ntract to s in arbitrary	entation n, an integer e owner set the user to 23	https://gith m/BlockCha urity/Ether /tree/maste VVIZIOToke https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md	insSec Fokens r/SER n, ub.co insSec Fokens er/GE int%2	A-Ser- Servv/01- 08- 18/287
Sexhdsolo Proj	ject							
Sexhdsolo Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for sexhdsolo, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13716			https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi 0integer%20 low.md, https://gith m/BlockCha urity/Ether /tree/maste hdsolo	insSec Fokens er/GE int%2 Doverf ub.co insSec Fokens	A-Sex- Sexhd/01 -08- 18/288
CV Scoring Scale (CV	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

 Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Sharktech Pro	ject				
Sharktech					
Overflow	12-07-2018	5	AnintegeroverflowvulnerabilityexistsinthefunctionbatchTransferofSHARKTECH(SKT),anEthereumtokensmartcontract.An attacker could useittosetanyuser'sbalance.CVE-ID:CVE-2018-14001	https://github.co m/VenusADLab/E therTokens/blob/ master/SHARKTE CH/SHARKTECH. md	A-Sha- Shark/01 -08- 18/289
Soscoin Projec	t				
Soscoin					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for SOSCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13681	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/SOS Coin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Sos- Sosco/01- 08- 18/290
Stctoken Proje	ct				
Stctoken					1
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for STCToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13745	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/STC Token, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Stc- Stcto/01- 08- 18/291
Superenergy P	roject				
Superenergy					

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-SOL Injection; XSS- Cross Site Scripting;									
sqr-sqL injection; x55- ci oss site script	ing;								

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for SuperEnergy (SEC), an Ethereum token, has an intege overflow that allows the owne of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13743	 m/BlockChainsSec urity/EtherTokens r /tree/master/SEC, r e https://github.co 	A-Sup- Super/01 -08- 18/292
Theflashtoken	Project				
Theflashtoken					
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for TheFlashToken, an Ethereum token, has an intege overflow that allows the owne of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13772	 m/BlockChainsSec urity/EtherTokens r /blob/master/GE mCHAIN/mint%2 0integer%20overf 	A-The- Thefl/01- 08- 18/293
Thread Projec	t				
Thread					I
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Thread, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance o an arbitrary user to any value CVE-ID:CVE-2018-13752	 m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 f 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Thr 	A-Thr- Threa/01 -08- 18/294
Tickets Projec	•			ead	
	•				
Tickets					

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference,	Patch	NCIIPC ID
Overflow	09-07-2018	5	smart contra for tickets (token, has a that allows contract to an arbitrary	oken functio act implemer TKT), an Eth an integer ov the owner set the bala v user to any 5-2018-1374	ntation ereum erflow of the nce of value.	https://gith m/BlockCha urity/Ether' /tree/maste ets, https://gith m/BlockCha urity/Ether' /blob/maste MCHAIN/m 0integer%2 low.md	ainsSec Tokens er/tick ub.co ainsSec Tokens er/GE int%2	A-Tic- Ticke/01 08- 18/295
<u>Fokenmachu P</u>	roject							
<u>Tokenmachu</u> Overflow	09-07-2018	5	smart contra for Tok Ethereum to overflow tha of the cor balance of a any value.	oken functio act implemer cenMACHU, oken, has an i at allows the ntract to se in arbitrary u C-2018-1373	ntation an nteger owner et the user to	https://gith m/BlockCha urity/Ether' /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha urity/Ether' /tree/masta enMACHU	ainsSec Tokens er/GE int%2 Ooverf ub.co ainsSec Tokens	A-Tok- Token/01 -08- 18/296
Tradesman Pro	oject							
Tradesman								
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Tradesman, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13713		https://gith m/BlockCha urity/Ether' /tree/maste desman, https://gith m/BlockCha urity/Ether' /blob/mast MCHAIN/m Ointeger%2 low.md	ainsSec Tokens er/Tra ub.co ainsSec Tokens er/GE int%2	A-Tra- Trade/01 -08- 18/297	
Tube Project								
		3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Descrij	ption & CVE	ID	Reference	/Patch	NCIIPC ID
Tube								
Overflow	09-07-2018	5	for Tube, a has an inte allows the contract to an arbitrary	art contract implementation Tube, an Ethereum token, an integer overflow that			ub.co ainsSec Tokens er/Tub ub.co ainsSec Tokens er/GE int%2 0overf	A-Tub- Tube/01- 08- 18/298
Ublasti Project	t							
Ublasti								
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Ublasti, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13763		ntation token, w that of the ance of v value. 53	https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha urity/Ether /tree/maste asti	ainsSec Tokens er/GE int%2 Ooverf ub.co ainsSec Tokens	A-Ubl- Ublas/01- 08- 18/299
Ultimatecoin P	roject							
Ultimatecoin								
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for UltimateCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13770		https://gith m/BlockCha urity/Ether /blob/mast MCHAIN/m 0integer%2 low.md, https://gith m/BlockCha	ainsSec Tokens er/GE int%2 0overf ub.co ainsSec	A-Ult- Ultim/01- 08- 18/300	
		3-4	4-5	5-6		urity/Ether /tree/maste mateCoin 7-8		9-10
CV Scoring Scale (CV	UCC)	J-1	T -J	0.0	0 /		0-5	110

Vulnerability Type(s)	Publish Date	CVSS	Descrip	tion & CVE	ID	Reference/	Patch	NCIIPC ID
Utbtokentest P	roject							
Utbtokentest								
Overflow	09-07-2018	5	smart contra	TokenTest, oken, has an at allows the atract to s n arbitrary	entation an integer e owner set the user to	https://githu m/BlockCha urity/Ether7 /tree/maste TokenTest, https://githu m/BlockCha urity/Ether7 /blob/maste MCHAIN/mi 0integer%20 low.md	insSec Fokens r/UTB ub.co insSec Fokens er/GE nt%2	A-Utb- Utbto/01- 08- 18/301
Vanminhcoin H	Project							
Vanminhcoin								
Overflow	09-07-2018	5	The mintT smart contra for VanMinh token, has a that allows contract to an arbitrary CVE-ID:CVE	Coin, an Et n integer o the owner set the bal user to an	entation hereum verflow of the ance of y value.	https://githu m/BlockCha urity/Ether7 /blob/master MCHAIN/mi 0integer%20 low.md, https://githu m/BlockCha urity/Ether7 /tree/master MinhCoin	insSec Fokens er/GE nt%2 Doverf ub.co insSec Fokens	A-Van- Vanmi/01 -08- 18/302
Vitemoneycoir								
<u>Vitemoneycoin</u> Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for ViteMoneyCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13682			https://githu m/BlockCha urity/EtherT /tree/maste MoneyCoin, https://githu m/BlockCha urity/EtherT /blob/maste MCHAIN/mi 0integer%20	insSec Fokens r/Vite ub.co insSec Fokens er/GE nt%2	A-Vit- Vitem/01 -08- 18/303
CV Scoring Scale (CV	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID		
						low.md				
Vornoxcointok	en Project									
Vornoxcointoke										
Overflow	09-07-2018	5	The mintT smart contra for Vornox Name: Vorn Ethereum to overflow that of the cor balance of a any value. CVE-ID:CVE	(VRX) (C noxCoinTok oken, has an at allows the ntract to s in arbitrary	entation Contract en), an integer e owner set the user to	https://gith m/BlockCha urity/Ether /tree/maste nToken, https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi Ointeger%20 low.md	insSec Fokens r/Coi ub.co insSec Fokens er/GE nt%2	A-Vor- Vorno/01 -08- 18/304		
Wemediachain Project										
Wemediachain										
Overflow	12-07-2018	5	vulnerability	y exists batchTransf ain (WMG token attacker co ny user's l	C), an smart ould use oalance.	https://gith m/VenusAD therTokens/ master/WeM hain%28WM 9, https://gith m/VenusAD therTokens/ master/SHA CH/SHARKT md	Lab/E /tree/ /dediaC /AC%2 ub.co Lab/E /blob/ RKTE	A-Wem- Wemed/0 1-08- 18/305		
Worldopctionc	•									
Worldopctioncl										
Overflow	09-07-2018	5	smart contra	OpctionCha oken, has an at allows the ntract to s n arbitrary	entation in, an integer e owner set the user to	https://gith m/BlockCha urity/Ether /tree/maste ldOpctionCh https://gith m/BlockCha urity/Ether /blob/maste MCHAIN/mi	insSec Fokens r/Wor ain, ub.co insSec Fokens er/GE	A-Wor- World/01 -08- 18/306		
CV Scoring Scale (CV	/\$\$)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		

 CV Scoring Scale (LVSS)

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

 Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE ID	Reference/Patch	NCIIPC ID
190009					0integer%20overf low.md	
Yambyo Projec	t					
Yambyo						
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for YAMBYO, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13675		https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/YA MBYO, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	1-08- 18/307
Ylctoken Proje	ct					
Ylctoken						
Overflow	09-07-2018	5	smart contra for YLCTol- token, has a that allows contract to an arbitrary	oken function of a act implementation ken, an Ethereum an integer overflow the owner of the set the balance of v user to any value. 2-2018-13779	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/YLC Token	08- 18/308
Yss Project						
YSS Overflow	09-07-2018	5	smart contra for YSS, an has an inte allows the contract to an arbitrary	oken function of a act implementation Ethereum token, eger overflow that e owner of the set the balance of v user to any value. C-2018-13707	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/YSS, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2	08- 18/309
CV Scoring Scale (CVSS)		3-4	4-5	5-6 6-7	7-8 8-	9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Descrip	otion & CVE	EID	Reference/	Patch	NCIIPC ID
						0integer%20 low.md)overf	
Yumerium Pro	ject							
Yumerium	1							
Overflow	09-07-2018	5	The mintT smart contra for Yumeri token, has a that allows contract to an arbitrary CVE-ID:CVE	um, an Et in integer o the owner set the bal user to an	entation hereum verflow of the lance of y value.	https://githu m/BlockCha urity/EtherT /blob/maste MCHAIN/mi 0integer%20 low.md https://githu	insSec Fokens er/GE nt%2 Doverf	A-Yum- Yumer/0 1-08- 18/310
						m/BlockCha urity/EtherT /tree/maste merium	insSec Cokens	
Zip Project								
ZIP								
Overflow	09-07-2018	5	smart contra for ZIP, an has an inte	Ethereum eger overflo owner set the bal	entation token, ow that of the lance of y value.	https://githu m/BlockCha urity/EtherT /tree/maste https://githu m/BlockCha urity/EtherT /blob/maste MCHAIN/mi 0integer%20 low.md	insSec Tokens r/ZIP, ub.co insSec Tokens er/GE nt%2	A-Zip- ZIP/01- 08- 18/311
Zpecoin Projec	zt							
Zpecoin	00.07.0010	-				1	, ,	. 7
Overflow	09-07-2018	5	The mintT smart contra for ZPEcoi token, has a that allows contract to an arbitrary CVE-ID:CVE	n, an Et in integer o the owner set the bal user to an	entation hereum werflow of the lance of y value.	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/ZPE coin, https://github.co m/BlockChainsSec		A-Zpe- Zpeco/01 -08- 18/312
						urity/EtherT /blob/maste MCHAIN/mi	Cokens er/GE nt%2	
CV Scoring Scale (C		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 Forg	ery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;
Sql-SQL Injection; XSS- Cross Site Script	ing;						

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				0integer%20overf low.md	
Ztoken Project					
Ztoken					
Overflow	09-07-2018	5	The mintToken function of smart contract implementation for ZToken, an Ethereu token, has an integer overflow that allows the owner of the contract to set the balance an arbitrary user to any value CVE-ID:CVE-2018-13768	on m/BlockChainsSec m urity/EtherTokens w /blob/master/GE ne MCHAIN/mint%2 of 0integer%20overf le. low.md,	A-Zto- Ztoke/01- 08- 18/313
				https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/ZTo ken	
			Hardware		
ARM,Intel					
			eron J,Celeron N,Core I3,Cor 1 J,Pentium N,Xeon,Xeon Bron		ore M3,Core
Overflow Gain Information	10-07-2018	4.7	Systems wi microprocessors utilizin speculative execution an branch prediction may allo unauthorized disclosure information to an attack with local user access via speculative buffer overflo and side-channel analys CVE-ID:CVE-2018-3693	th https://www.suse. ng com/support/kb/ nd doc/?id7023075, w of https://thehacker er news.com/2018/0 a 7/intel-spectre- w vulnerability.html,	H-ARM- Atom/01- 08- 18/314
			Operating System (OS)		
Oracle					
Solaris					
DoS	18-07-2018	4.3	Vulnerability in the Solar component of Oracle Su Systems Products Sui (subcomponent: Kerne Supported versions that a affected are 10 and 11 Difficult to explo	in te l). re 2.	0-0ra- Solar/01- 08- 18/315
CV Scoring Scale (C)		3-4	4-5 5-6 6	-7 7-8 8-9	9-10

CV Scoring Scale (CVSS)	3-4	4-5	5-0	0-7	7-0	0-9	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)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via DHCP 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 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:N/I:N/A:L). CVE-ID:CVE-2018-2901		
NA	18-07-2018	4.9	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11.3. Easily exploitable 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 access to critical data or complete access to all Solaris accessible data. CVSS 3.0 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI :N/S:U/C:H/I:N/A:N). CVE-ID:CVE-2018-2903	NA	0-0ra- Solar/01- 08- 18/316
NA	18-07-2018	6.8	CVE-ID:CVE-2018-2903Vulnerability in the Solariscomponent of Oracle SunSystems Products Suite(subcomponent: Kernel). Thesupported version that isaffected is 11.3. Easilyexploitable vulnerabilityallows low privileged attacker	NA	0-0ra- Solar/01- 08- 18/317

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;									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			with network access via RPC 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 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-2018-2908		
NA	18-07-2018	7.2	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Availability Suite Service). Supported versions that are affected are 10 and 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 takeover of Solaris. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI: N/S:U/C:H/I:H/A:H). CVE-ID:CVE-2018-2892	NA	0-0ra- Solar/01- 08- 18/318
NA	18-07-2018	8	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: NVIDIA-GFX Kernel driver). The supported version that is affected is 11.3. Easily exploitable vulnerability	NA	0-0ra- Solar/01- 08- 18/319

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Sql-SQL Injection; XSS- Cross Site Script		gery; Dir. Trav	vDirectory Tr	aversal; DoS-	Denial of Serv	ice; NA- Not A	pplicable;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			allows low privileged attacker with network access via ISCSI 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 as well as unauthorized update, insert or delete access to some of Solaris accessible data and unauthorized read access to a subset of Solaris accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:H). CVE-ID:CVE-2018-2926		
NA	18-07-2018	8.8	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: 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 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	NA	0-0ra- Solar/01- 08- 18/320

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;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:U/C:H/I:H/A:N). CVE-ID:CVE-2018-2928		

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;											