(Notice)	National Critical Information Infrastructure Protection Centre CVE Report CV Scoring Scale: 3-10 15 Oct -15 Nov 2018 Vol. 05 No.21									
Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Pa	atch NCIII	PC ID				
			Application							
Catfish-cms										
Catfish Blog										
CSRF	29-10-2018	6.8	A CSRF issue was discovered admin/Index/tiquan in cat blog 2.0.33. CVE-ID:CVE-20 18735	fish m/AvaterXXX	/catf Catfi, ter/c 11-18	/19-				
Catfish Cms										
CSRF	29-10-2018	6.8	A CSRF issue was discovered admin/Index/addmanageuser ml in Catfish CMS 4.8.30. CID:CVE-2018-18734	ht m/AvaterXXX	/catf Catfi, ter/c 11-18	/19-				
IBM				<u>.</u>						
Rational Quality	Manager									
XSS	02-11-2018	3.5	IBM Quality Manager (RQM) through 5.0.2 and 6.0 through 6.0.6 are vulnerable to cross-scripting. This vulnerable allows users to embed arbitr JavaScript code in the Web thus altering the intenfunctionality potentially lead to credentials disclosure with trusted session. IBM X-Force 132929. CVE-ID:CVE-2017-16	xforce.ibmclor site m/vulnerabili ility 132929 rary O UI ided ding in a ID:	ud.co Ratio	/19-				
Websphere Comm	nerce									
XSS	24-10-2018	3.5	IBM WebSphere Comme Enterprise V7, V8, and V9 vulnerable to cross-site script This vulnerability allows user embed arbitrary JavaScript c in the Web UI thus altering intended functionality potenti leading to credentials disclos	xforce.ibmclor ting. m/vulnerabilities to 142596 code the https://www.ially com/support/ sure view.wss?uid=	ibm.	sp/19-				
			within a trusted session. IBM Force ID: 142596. CVE-ID:C 2018-1541							
CV Scoring Scale (CVSS		3-4	4-5 5-6 6 ery; Dir. TravDirectory Traversal; Dos	7-8	8-9	9-10				

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description	& CVE ID		Reference	e/Patch	NCIIPC ID
Oracle								
NA NA	16-10-2018	4.3	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Utility). The supported version that is affected is Java SE: 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). CVE-ID:CVE-				ourity.n a/adviso 3-0001/ ccess.red errata/R	A-Ora- JDK,J/19- 11-18/5
Mysql			2018-3150					
NA NA	16-10-2018	4	Vulnerability in the MySQL https://usn.ubunt server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to https://lists.debia n.org/debian-lts-				A-Ora- Mysql/19- 11-18/6	
CV Scoring Scale (CVS	SS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s) Injection; XSS- Cross	: CSRF-Cross Site Re	quest Forg	ery; Dir. TravDi	rectory Traver	sal; DoS-Den	ial of Service; l	NA- Not App	licable; Sql-SQL

Vulnerability	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Type(s)					
			compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). CVE-ID:CVE-2018-3143	announce/2018/1 1/msg00007.html	
NA	16-10-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). CVE-ID:CVE-2018-3156	https://usn.ubunt u.com/3799-1/ https://security.n etapp.com/adviso ry/ntap- 20181018-0002/ https://lists.debia n.org/debian-lts- announce/2018/1 1/msg00007.html	A-0ra- Mysql/19- 11-18/7
NA	16-10-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low	https://usn.ubunt u.com/3799-1/ https://security.n etapp.com/adviso ry/ntap- 20181018-0002/	A-0ra- Mysql/19- 11-18/8

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

Vulnerability	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Type(s)			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	https://lists.debia n.org/debian-lts- announce/2018/1 1/msg00007.html	
			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-2018-3251		
NA	16-10-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). CVE-ID:CVE-2018-3133	https://lists.debia n.org/debian-lts- announce/2018/1 1/msg00004.html https://security.n etapp.com/adviso ry/ntap- 20181018-0002/ https://usn.ubunt u.com/3799-1/ https://usn.ubunt u.com/3799-2/	A-0ra- Mysql/19- 11-18/9
NA	16-10-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior,	https://lists.debia n.org/debian-lts- announce/2018/1 1/msg00004.html https://lists.debia	A-0ra- Mysql/19- 11-18/10

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	e/Patch	NCIIPC ID
			vulnerability privileged att access via m compromise	allows allows acker with ultiple pro MySQL attacks can reability to quently reete DOS) of 3.0 Base Simpacts)	rploitable high network tocols to Server. of this esult in cause a epeatable of MySQL Score 4.9 . CVSS	announce 1/msg000 https://u u.com/37 https://u u.com/37	2018/1 2007.html sn.ubunt 99-2/ sn.ubunt 99-1/ ecurity.n	
Pivotal Software			2010 0202					
Spring Security C	Dauth							
NA	18-10-2018	6.8	modify the authorization a privilege subsequent scenario car application is custom appredeclares Authorization a controller	3.4, and 2.2 prior to 2 2.0.16, and versions to a under malicious craft a requadopoint the previously request an escalation approval an happen configured oval endpoint approval endpoint endpoint approval endpoint endpoint approval endpoint endpoi	2 prior to 2.1.3, and and older could be privilege certain user or est to the hat can y saved ad lead to on the lato use a point that equest as rgument. exposes all of the exposes all of the exposes all of the lato.	https://p security/c 2018-157	cve-	A-Piv- Sprin/19- 11-18/11

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Server (e.g. @EnableAuthorizationServer) and use a custom Approval Endpoint that declares AuthorizationRequest as a controller method argument. This vulnerability does not expose applications that: Act in the role of an Authorization Server and use the default Approval Endpoint, act in the role of a Resource Server only (e.g. @EnableResourceServer), act in the role of a Client only (e.g. @EnableOAuthClient). CVE-ID:CVE-2018-15758		
Sem-cms					
Semcms					
CSRF	29-10-2018	6.8	A CSRF issue was discovered in SEMCMS 3.4 via the admin/SEMCMS_User.php?Class= add&CF=user URI. CVE-ID:CVE-2018-18742	https://github.co m/AvaterXXX/SE MCMS/blob/mast er/CSRF.md	A-Sem- Semcm/19- 11-18/12
Wuzhicms					
Wuzhi Cms					
CSRF	29-10-2018	6.8	An issue was discovered in WUZHI CMS 4.1.0. There is a CSRF vulnerability that can change the super administrator's password via index.php?m=core&f=panel&v=e dit_info. CVE-ID:CVE-2018-18711		A-Wuz- Wuzhi/19- 11-18/14
CSRF	29-10-2018	6.8	An issue was discovered in WUZHI CMS 4.1.0. There is a CSRF vulnerability that can change the super administrator's username via index.php?m=member&f=index&v=edit&uid=1. CVE-ID:CVE-2018-18712	https://github.co m/wuzhicms/wuz hicms/issues/156	A-Wuz- Wuzhi/19- 11-18/15

	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									
ı	Injection: XSS- Cross Site Scripting:									

9-10

Vulnerability	Publish Date	CVSS	Description & CVE ID	Reference	e/Patch	NCIIPC ID
Type(s)						
XSS	05-11-2018	3.5	An issue was discovered	1 ,, 0		A-Wuz-
			WUZHI CMS 4.1.0. There is store	,	,	Wuzhi/19-
				in hicms/issu	ies/158	11-18/16
			1 1	ria to		
			details/open/ within a secon			
			input field. CVE-ID:CVE-201			
			18938			
Wuzhi Cms Proj	ect					
Wuzhi Cms						
XSS	05-11-2018	3.5	An issue was discovered	in https://git	thub.co	A-Wuz-
			WUZHI CMS 4.1.0. There is store	,	,	Wuzhi/19-
				in hicms/issu	ues/159	11-18/13
			index.php?m=core&f=index via			
			seventh input field. CVE-ID:CV 2018-18939	E-		
	An	nlicatio	2018-18939 n Operating System (Application	on OS)		
Oracle,Redhat	Пр	pricacio	n operating system (Application	JII,03)		
•	ux Deskton Ent	ernrise	Linux Server,Enterprise Lin	uix Server l	Eus Enteri	nrise Linux
Workstation,JDK	and the second s	er prise	Elitax Server, Eliter prise Elit	iux Scivei I	из,шпсет [prise Elliax
NA	16-10-2018	5.1	Vulnerability in the Java SE, Ja	va https://ac	cess.red	A-Ora-
			SE Embedded component			Enter/19-
			Oracle Java SE (subcomponer		:3521	11-18/21
			Hotspot). Supported version			
			that are affected are Java S	,	,	
			7u191, 8u182 and 11; Java S			
			Embedded: 8u181. Difficult	1 //		
			exploit vulnerability allow	,		
			unauthenticated attacker winetwork access via multip			
			protocols to compromise Java S			
			Iava SE Embedded. Successi		,	
			attacks require huma	1 //		
			interaction from a person oth	,	,	
			than the attacker and while the			
			vulnerability is in Java SE, Java S	SE HSA-2018	:3409	
			Embedded, attacks m	1 , ,	-	
			significantly impact addition		/adviso	
			products. Successful attacks		0004 /	
			this vulnerability can result			
			takeover of Java SE, Java S Embedded. Note: Th	SE https://ac nis hat.com/e		
	<u> </u>	3-4	4-5 5-6 6-7	,	8-9	9-10
CV Scoring Scale (CVS	S)	3-4	4-5 5-6 6-7	7-8	8-9	9-10
Vulnerability Type(s)	: CSRF-Cross Site Re	quest Forg	ery; Dir. TravDirectory Traversal; DoS-l	Denial of Service; I	NA- Not Appl	icable; Sql-SQL

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID			Reference	e/Patch	NCIIPC ID
Enterprise Line	ny Daskton Fr	tornrico	vulnerability Java deploy servers, that trusted code by an admit Base Score Integrity impacts). (CVSS:3.0/A'/S:C/C:H/I:H 2018-3169	s, typically andboxed Janions or sali untrusted comes from the design of	in clients ava Web andboxed E 8), that code (e.g. om the the Java y. This apply to bically in run only installed CVSS 3.0 dentiality, vailability Vector: R:N/UI:RE-ID:CVE-	HSA-2018 https://ac hat.com/e HSA-2018 https://ac	cess.red rrata/R :3533 cess.red rrata/R :3003 cess.red rrata/R :3000 cess.red rrata/R :3350 cess.red rrata/R :3002 cess.red rrata/R :3002 cess.red rrata/R :3001 ww.debi curity/2 :326	vrico Linuv
Workstation, JDK DoS	and the second s	5	Vulnerability SE Embedde of Oracle Jave Sound). Supare affected 7u191 and Embedded: R28.3.19. vulnerability unauthentica network approtocols to Java SE Successful vulnerability unauthorized partial denis	cy in the Jav. d, JRockit co a SE (subco ported vers are Java SI 8u182; 8u181; Easily ex ated attack ccess via compromise compromise Embedded, attacks can red d ability to	a SE, Java omponent omponent: ions that E: 6u201, Java SE JRockit: eploitable allows er with multiple e Java SE, JRockit. of this esult in cause a e (partial	https://ww an.org/sec 018/dsa-4 https://us u.com/380	ww.debi curity/2 .326 n.ubunt 04-1/ cess.red rrata/R :3533 curity.n /adviso -0001/ cess.red rrata/R :3534 cess.red rrata/R	A-Ora- Enter/19- 11-18/17
CV Scoring Scale (CVS	S)	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
Туре(з)			Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). CVE-ID:CVE-2018-3214	https://access.red hat.com/errata/R HSA-2018:3409 https://access.red hat.com/errata/R HSA-2018:3003 https://access.red hat.com/errata/R HSA-2018:3007 https://access.red hat.com/errata/R HSA-2018:3008 https://access.red hat.com/errata/R HSA-2018:3002 https://access.red hat.com/errata/R HSA-2018:3001 https://access.red hat.com/errata/R HSA-2018:2943 https://access.red hat.com/errata/R HSA-2018:2942 https://access.red hat.com/errata/R HSA-2018:2942 https://access.red hat.com/errata/R HSA-2018:2942 https://access.red hat.com/errata/R HSA-2018:2942 https://access.red hat.com/errata/R HSA-2018:3000	
DoS	16-10-2018	6.8	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	https://access.red hat.com/errata/R HSA-2018:3007 https://access.red hat.com/errata/R HSA-2018:2942 https://access.red hat.com/errata/R HSA-2018:3000 https://www.debi an.org/security/2 018/dsa-4326 https://usn.ubunt u.com/3824-1/ https://usn.ubunt u.com/3804-1/	A-Ora- Enter/19- 11-18/18
CV Scoring Scale (CVS		3-4	4-5 5-6 6-7 ery; Dir. TravDirectory Traversal; DoS-Den	7-8 8-9	9-10

Type(s)		Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This	https://security.n etapp.com/adviso ry/ntap- 20181018-0001/ https://access.red hat.com/errata/R HSA-2018:3350 https://access.red hat.com/errata/R HSA-2018:3409 https://access.red hat.com/errata/R HSA-2018:3521 https://access.red hat.com/errata/R HSA-2018:3533 https://access.red hat.com/errata/R	
		vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). CVE-ID:CVE-2018-3180	HSA-2018:3001 https://access.red hat.com/errata/R HSA-2018:3002 https://access.red hat.com/errata/R HSA-2018:3534 https://access.red hat.com/errata/R HSA-2018:3008 https://access.red hat.com/errata/R HSA-2018:3003 https://access.red hat.com/errata/R	
NA 16-10	D-2018 5.1	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows	https://usn.ubunt u.com/3804-1/ https://access.red hat.com/errata/R HSA-2018:3534 https://www.debi an.org/security/2 018/dsa-4326 https://usn.ubunt	A-Ora- Enter/19- 11-18/19
CV Scoring Scale (CVSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10

Vulnerability	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Type(s)					
			unauthenticated attacker with	u.com/3824-1/	
			network access via multiple	https://access.red	
			protocols to compromise Java SE,	hat.com/errata/R	
			Java SE Embedded, JRockit.	HSA-2018:3521	
			Successful attacks require human	https://access.red	
			interaction from a person other	hat.com/errata/R	
			than the attacker and while the	HSA-2018:3533	
			vulnerability is in Java SE, Java SE	https://security.n	
			Embedded, JRockit, attacks may	etapp.com/adviso	
			significantly impact additional	ry/ntap-	
			products. Successful attacks of	20181018-0001/	
			this vulnerability can result in	https://access.red	
			takeover of Java SE, Java SE	hat.com/errata/R	
			Embedded, JRockit. Note: This	HSA-2018:3000	
			vulnerability applies to Java	https://access.red	
			deployments, typically in clients	hat.com/errata/R	
			running sandboxed Java Web	HSA-2018:3409	
			Start applications or sandboxed	https://access.red	
			Java applets (in Java SE 8), that	hat.com/errata/R	
			load and run untrusted code (e.g.	HSA-2018:3008	
			code that comes from the	https://access.red	
			internet) and rely on the Java	hat.com/errata/R	
			sandbox for security. This	HSA-2018:3002	
			vulnerability can also be	https://access.red	
			exploited by using APIs in the	hat.com/errata/R	
			specified Component, e.g. through	HSA-2018:3003	
			a web service which supplies data	https://access.red	
			to the APIs. CVSS 3.0 Base Score	hat.com/errata/R	
			8.3 (Confidentiality, Integrity and	HSA-2018:3007	
			Availability impacts). CVSS		
			Vector:	hat.com/errata/R	
			(CVSS:3.0/AV:N/AC:H/PR:N/UI:R	HSA-2018:2943	
			/S:C/C:H/I:H/A:H). CVE-ID:CVE-	https://access.red	
			2018-3149	hat.com/errata/R	
				HSA-2018:3350	
				https://access.red	
				hat.com/errata/R	
				HSA-2018:3001	
				https://access.red	
				hat.com/errata/R	
				HSA-2018:2942	
				113A-2010:2742	

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

Vulnerability	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Type(s)					
NA	16-10-2018	6.8	Vulnerability in the Java SE, Java	https://access.red	A-Ora-
			SE Embedded, JRockit component	hat.com/errata/R	Enter/19-
			of Oracle Java SE (subcomponent:	HSA-2018:3002	11-18/20
			Scripting). Supported versions	https://www.debi	
			that are affected are Java SE:	an.org/security/2	
			8u182 and 11; Java SE	018/dsa-4326	
			Embedded: 8u181; JRockit:	https://usn.ubunt	
			R28.3.19. Difficult to exploit	u.com/3804-1/	
			vulnerability allows	https://access.red	
			unauthenticated attacker with	hat.com/errata/R	
			network access via multiple	HSA-2018:3521	
			protocols to compromise Java SE,	https://access.red	
			Java SE Embedded, JRockit. While	hat.com/errata/R	
			the vulnerability is in Java SE,	HSA-2018:3534	
			Java SE Embedded, JRockit,	https://security.n	
			attacks may significantly impact	etapp.com/adviso	
			additional products. Successful	ry/ntap-	
			attacks of this vulnerability can	20181018-0001/	
			result in takeover of Java SE, Java	https://access.red	
			SE Embedded, JRockit. Note: This	hat.com/errata/R	
			vulnerability applies to Java	HSA-2018:3003	
			deployments, typically in clients	https://access.red	
			running sandboxed Java Web	hat.com/errata/R	
			Start applications or sandboxed	HSA-2018:3533	
			Java applets (in Java SE 8), that	https://access.red	
			load and run untrusted code (e.g.	hat.com/errata/R	
			code that comes from the	HSA-2018:2943	
			internet) and rely on the Java	1 , ,	
				hat.com/errata/R	
			vulnerability can also be	HSA-2018:2942	
			exploited by using APIs in the		
			specified Component, e.g. through		
			a web service which supplies data		
			to the APIs. CVSS 3.0 Base Score		
			9.0 (Confidentiality, Integrity and		
			Availability impacts). CVSS		
			Vector:		
			(CVSS:3.0/AV:N/AC:H/PR:N/UI:N		
			/S:C/C:H/I:H/A:H). CVE-ID:CVE-		
			2018-3183		

	2.4	4-5	5.6	6.7	7-Ω	8-9	9-10
CV Scoring Scale (CVSS)	3-4	4-3	3-0	0-7	/-0	0-9	9-10