13

SOAP WSDL Parser SQL Code Execution

Share:

State	Resolved (Closed)
Disclosed	**January 17, 2019 12:46am +0530**
Reported To	U.S. Dept Of Defense
Weakness	SQL Injection
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

SUMMARY BY U.S. DEPT OF DEFENSE

A critical SOAP WSDL Parser SQL Code Execution vulnerability (assigned CVE-2018-16803) was discovered on a Department of Defense (DoD) website by Joel Aviad Ossi. If properly exploited this could have resulted in the complete loss of the website and the underlining information system. Researcher websecnl was able to expertly demonstrate this vulnerability to the DoD's Vulnerability Disclosure Program (VDP), and it was rapidly mitigated by the system owner. Very well done websecnl, thank you!

DoD VDP Team

TIMELINE

websecnl submitted a report to **U.S. Dept Of Defense**. Aug 4th (6 months ago)

Summary:
SOAP WSDL Parser SQL Code Execution

Description:
It was possible to parse WSDL resources and read all functions from the SOAP Admin Panel, therefor i was able to repeat the sql query with a tampered request with my own custom SQL command.
i was able to extract all the database names for PoC, there is no doubt in my mind that i could login to the admin panel and compromise the entire DoD Information System.

Impact

Remote Code Execution

Step-by-step Reproduction Instructions

1. Visit:[redacted] and go to the staff links 'CIMScan' Image: [redacted]/34570b2eaa899ae001e1bc666be3546a.png
2. [redacted]/c400bc1369bddeca580646b14c38a562.png
3. [redacted]/32e085f593bfbf8599359d968cf52dc0.png

Product, Version, and Configuration (If applicable)

Web Application

Suggested Mitigation/Remediation Actions

I will report it to CIMScan since i am not sure if this affect's your code, it might very well be the code of CIMScan which in that case you will need to remove it from your website to prevent employees from being compromised.

Impact

Remote Code Execution

BOT: U.S. Dept Of Defense posted a comment. Aug 4th (6 months ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at @DeptofDefense.

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team

websecnl posted a comment. Aug 4th (6 months ago)

Please note that this problem might be on the side of cimtechniques.com , if the DoD Devops team will contact them regarding this i would like to be mentioned as the finder of this vulnerability and would like you to ask them to publish the information regarding this vulnerability once its patched and cooperation in requesting a CVE number for this finder since it probably affects thousands of other customers who use CIMScan.

This is the ethical and fair thing to do, i hope you can understand.

Once you did that please add the CVE number as reference to this report and if possible make it public with limited view on hackerone. :) i asked you before to make some of my reports public but you never did.

websecnl posted a comment. Updated Jan 16th (19 hrs ago)

Ok i can confirm it is DoD property, the server name returns: [redacted]

i recognize [redacted] is the DoD institute name.

i also contacted CIMScan regarding a possible flaw in their software in order to maybe claim a CVE number. (no worries i will not give them any information regarding the flaw in your system obviously!)

websecnl posted a comment. Updated Jan 16th (19 hrs ago)

[redacted]

[redacted]
[redacted]

[redacted]/3b81cbae3830a65089a87043805a39b7.png

I[redacted]

Kind Regards,
Joel Aviad Ossi
websecnl

websecnl posted a comment. Updated Jan 16th (19 hrs ago)

^ after digging [redacted]

[redacted]

Tought you should know.

websecnl posted a comment. Updated Jan 16th (19 hrs ago)

[redacted]

[redacted]

ag3nt-z3 posted a comment. Updated Jan 16th (19 hrs ago)

@websecnl how did you get a system name of [redacted]

I'm seeing an IP of [redacted] and i'm not resolving a hostname like that.

websecnl posted a comment. Updated Jan 16th (18 hrs ago)

See attached picture for how i fetched that name.
note that you need wsdler burp suite plugin in order to replicate this.

i know the IP looks like its out of scope but the wired thing is this:
[redacted] <-- subdomain starts with '[redacted]' and the system name i managed to fetch from that server [redacted]
'[redacted]' [redacted] also contains it.

it cant be a coincidence.... can it?

ag3nt-z3 updated the severity to Critical. Aug 10th (5 months ago)

ag3nt-z3 changed the status to ○ **Triaged**. Aug 10th (5 months ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

ag3nt-z3 posted a comment. Aug 10th (5 months ago)

@websecnl I don't think you'll get a CVE out of this because it just seems horribly misconfigured. But, I'm rating it a critical because I was able to get a sqli through sqlmap. The injection is as 'sa' as the DBA, was able to enumerate the hostname you found, and could easily start taking this a lot further into the realm of getting a shell but there is no need, just stopping now and pushing it forward to get resolved.

Good find!
-Z3

websecnl posted a comment. Updated Jan 16th (19 hrs ago)

Than please make this report limited public once its resolved. :) many thanks!

As always, My pleasure.

[redacted]

ag3nt-j1 posted a comment. Updated Jan 17th (16 hrs ago)

@websecnl [redacted] Also wanted to say, good find. Your findings and reports have been getting better. Less [redacted] though, I'm going crazy over here with them ;)

websecnl posted a comment. Updated Jan 17th (16 hrs ago)

@ag3nt-j1 alright np, hahahah got 17 more [redacted]s for today, and in coming days i will report 24 more [redacted]s. after that (in the weekend) i will go on the hunt for something more interesting. Sorry... small things need to be solved too :p

ag3nt-z3 closed the report and changed the status to ○ **Resolved**. Aug 21st (5 months ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

websecnl posted a comment. Aug 22nd (5 months ago)

can you please publicly disclosure this finding.

websecnl posted a comment. Aug 24th (5 months ago)

any update regarding the disclosure of this report?

ag3nt-s21 posted a comment. Aug 24th (5 months ago)

@websecnl We are pushing it through the proper channels for public disclosure. Authorization to disclose has not yet been received.

websecnl posted a comment. Aug 24th (5 months ago)

Alright, i'll be waiting! Thanks!

websecnl posted a comment. Updated Sep 10th (4 months ago)

Hi fellas,

First of all, i would like to apologize for not being active latley, i promise to catchup and report more vulnerabilities soon.. it has been a busy couple of weeks for me at work (pentesting banks) we managed to get some big clients which usually means less free time.

Anyways, i would like to inform you that the CVE database has assigned this reference to this vulnerability: CVE-2018-16803

However this CVE will not have a public page until it will be disclosed by either you or simtechniques (for some reason simtechniques is not willing to comment, they dont deny or approve this vulnerability from ever existing... i guess some companies don't see the benefit of ethical hacking so your my only hope of receiving this CVE)

:) Please let me know if you added this CVE as a reference to this report and whenever you receive an update regarding permission for disclosure of this report.

Best Regards,
Joel Aviad Ossi

websecnl posted a comment. Updated Sep 13th (4 months ago)

:) Hi all, Sorry for bugging you with this again, but could you please make time to respond on the message above?

ag3nt-s21 posted a comment. Sep 13th (4 months ago)

@websecnl Sure, we can respond. You didn't exactly ask a question though. What would you like us to respond to? We do not publish CVE's, that's NIST. We also cannot request to publish this vulnerability until it has been mitigated by the system owner. If you're saying that Simtechniques isn't/wont comment or fix it, it may be a while before the system owner of this vulnerability can mitigate it effectively. Once they do, we'll let you know. It has been assigned a s verity level of 'Critical' so, they're aware of it and working toward a solution. Patience, young Padawan.

websecnl posted a comment. Updated Sep 13th (4 months ago)

haha, i have patience no worries, NIST already assigned this a number: "CVE-2018-16803" , my question / request is that once you publicly disclose this vulnerability if you could please include the CVE number as reference in the H1 public disclosure page since i am pretty sure Simtechniques won't add this to their blog.

basically NIST is waiting for a disclosure by either you (H1 Disclosure) or Simtechniques (Blog Disclosure), they assigned it a CVE but before it gets a public page on the NIST website they need a public disclosure page.

I understand that as long as simtechniques does not respond and due the severity of this vulnerability disclosure it might take some time and i respect that, but Simtechniques should keep in mind that there are rules to the H1 vulnerability disclosure
https://www.hackerone.com/disclosure-guidelines

If in 5 months from now the DoD stil will not hear anything back from Simtechniques than i would like to ask you to publicly disclose this report based on H1's Vulnerability Disclosure Last Resort process, unless you object to this ofcourse but thats a conversation for another time :)

Best Regards,
Joel Aviad Ossi

websecnl posted a comment. Nov 1st (3 months ago)

Hi guys,

Any update regarding publicly disclosing this?
it has been 2 months and there are no other vulnerable CIMScan 6.2 available online (searched through shodan & google)

2 months has been a reasonable amount of time and there is no direct indication of active exploitation of this vulnerability.

So could you please publicly disclose this and add its CVE to the reference "CVE-2018-16803"

Best Regards,
Joel

ag3nt-s21 posted a comment. Nov 1st (3 months ago)

@websecnl We understand your position but, until the system owner gives the OK to disclose (which the haven't done yet) we cannot disclose. Thanks for your patience.

websecnl posted a comment. Updated Jan 10th (7 days ago)

Dear sir/madam,

Thank you for your last reply.

I would like to remind you that the maximum deadline is approaching of the disclosure guidelines:

[1] `Last resort: If 180 days have elapsed with the Security Team being unable or unwilling to provide a vulnerability disclosure timeline, the contents of the Report may be publicly disclosed by the Finder. We believe transparency is in the public's best interest in these extreme cases.`

Please don't get me wrong, i am more than willing to wait even longer if its required however by the end of the month (when 6 months have passed) i have been more than 'patient' and could in theory disclose it myself in order to finally claim my CVE number which has been reserved for the past months.

But note that refusing to disclose this report + mention the CVE number as reference in disclosure after 6 months would be unreasonable towards me, this report has been resolved for a while now and it will no longer be fair to keep me waiting.

if you still believe this is a matter of national security and you insist on not disclosing this report than i am willing to extend the time but then i do want a disclosure timeline.

I hope you can understand that this is important for me as security researcher.

Thank you for understanding.

Best Regards,
Joel Aviad Ossi

Reference:
[1] https://www.hackerone.com/disclosure-guidelines

ag3nt-j1 posted a comment. Updated Jan 10th (7 days ago)

@websecnl I just want to point out that reporting to this program imposes guidelines and requirements that are clearly spelled out in our policy, I encourage you to review them https://hackerone.com/deptofdefense/ before disclosing anything without our permission. That being said, we are starting to do redacted disclosures and I have this report on the list to work. We will be reviewing this report to put through our disclosure process soon.

websecnl posted a comment. Jan 10th (7 days ago)

No worries, i was not planning on disclosing this report without your consent, i am aware of the guidelines and requirements that are spelled in your policy (I have been reporting to you since januari 2018). just wanted to remind you that i am still here waiting for this.

Excuse me if i sounded pushy or if i gave you the idea that i would disclosure this otherwise.

Just don't forget me please :) x

agent-1 posted a comment. Jan 10th (7 days ago)

@websecnl,
First of all I want to thank you for your vulnerability submission and making our websites more secure. While our policy does restrict all public disclosures prior to receiving explicit written consent from us, we are more than happy to approve your request. In addition to providing you with a redacted report here on H1 (in progress now) you can also put out the following:

"A critical SOAP WSDL Parser SQL Code Execution vulnerability was discovered on a Department of Defense (DoD) website. If properly exploited this could have resulted in the complete loss of the website and the underlining information system. Researcher websecnl was able to expertly demonstrate this vulnerability to the DoD's Vulnerability Disclosure Program (VDP), and it was rapidly mitigated by the system owner. Very well done websecnl, thank you!

DoD VDP Team"

Additionally, I would like to congratulate you publicly via twitter @DC3VDP. Please let me know if you would you have any issues with that?

websecnl posted a comment. Jan 10th (7 days ago)

@agent-1 That would be great, please use as name Joel Aviad Ossi (websecnl) instead of just websecnl :)
Would appriciate it allot.

It would be also great if you could include the CVE reference which was assigned to this vulnerability: CVE-2018-16803

Thank you so much in advance!

agent-1 posted a comment. Jan 10th (7 days ago)

Complete. Please be patient as we work on getting you a redacted report that you can publish. Thanks again!

websecnl posted a comment. Jan 10th (7 days ago)

Sure, Thank you :)

websecnl requested to disclose this report. Jan 11th (6 days ago)

Disclosure request, forgot to do this :)

By the way, thank you for the tweet.. this will help me allot in my career!

Best Regards,
Joel Aviad Ossi

ag3nt-j1 posted a comment. Jan 16th (18 hrs ago)

Hey Joel, I've gone through and redacted the report. just putting in a request to have the attachments removed through H1 and will publish.

Thanks again buddy.

ag3nt-j1 posted a comment. Jan 17th (17 hrs ago)

Joel, did you want limited or full disclosure on this. I can do either with the reactions I've made.

ag3nt-j1 agreed to disclose this report. Jan 17th (17 hrs ago)

This report has been disclosed. Jan 17th (17 hrs ago)

ag3nt-j1 posted a comment. Jan 17th (17 hrs ago)

Joel, I put it on for limited disclosure based on all the conversations back and forth. I've redacted quite a bit of the conversations and can do a full disclosure if you want. I just wanted to get this disclosed either way. If you change your mind let us know and we can do the full disclosure.

websecnl posted a comment. Updated Jan 17th (16 hrs ago)

redacted report is fine :)

but maybe you should redact the 'clickjackings' too since its no longer in scope and other people might think it is if they read this.

Thank you!