

From: s47F - personal privacy
To: s22(1)(a)(i) - irrelevant material
Cc: s22(1)(a)(ii) - irrelevant material
Subject: CAUTION: Email may contain unverified link [be careful if proceeding]Re: Log4j2 vulnerability
Date: Wednesday, 15 December 2021 2:10:32 PM

Just to clarify, references to Service Cloud in the below links, also imply Health Cloud - as they share the same underlying CRM platform.

Thanks,

s47F - personal privacy

Customer Success Director | Salesforce - Canberra, Australia

Mobile: s47F - personal privacy | Email: s47F - personal privacy

Follow us on:



On Wed, 15 Dec 2021 at 14:03, s47F - personal privacy wrote:

Hi s22(1)(a)(i) and team,

We have updated the public [status page](#) with a link to products we understand to be affected. The product list can be found here https://help.salesforce.com/s/articleView?language=en_US&type=1&id=000363736

Additionally, we have some advice as to whether you have noticed any log activity from Shield.

I am a Shield customer and I think I've observed exploitation in my logs, can you confirm?

- Public reports indicate high levels of scanning on the internet after the disclosure of this vulnerability. While this type of scanning can sometimes generate U-log events in which user agents are represented by exploit codes, Shield logs alone do not indicate proof of successful exploitation.
- Salesforce is actively monitoring this issue, and working to patch any of our services that either use the vulnerable component Log4j2 or provide it to customers. If we become aware of unauthorized access to customer data, we will notify impacted customers without undue delay.

I will send through updates as I see them. Any questions please let me know.

Thanks,

s47F - personal privacy

Customer Success Director | Salesforce - Canberra, Australia

Mobile: [s47F - personal privacy](#) | Email: [s47F - personal privacy](#)

Follow us on:    



On Mon, 13 Dec 2021 at 14:07, [s47F - personal privacy](#) wrote:

Hi 

Thanks for your time just now to discuss what we know about the Log4j2 vulnerability. As I mentioned on the call our Security team is still investigating, and as such, there is not a great detail of information to share at present. The below FAQ hopefully reassures the NDIA that we are actively protecting the NDIA's data.

At Salesforce, Trust is our #1 value, and we take the protection of our customers' data very seriously. We are aware of the recently disclosed Apache Log4j2 vulnerability (CVE-2021-44228). We are actively monitoring this issue, and are working to patch any Salesforce services that either use the vulnerable component Log4j2 or provide it to customers.

What is the impact?

- Salesforce currently has no evidence of unauthorized access to Salesforce systems or customer data due to this issue. Salesforce's investigation remains ongoing at this time.
- If Salesforce becomes aware of unauthorized access to Customer Data, we will notify impacted customers without undue delay.

Why did it take so long for you to alert us about this incident?

- Salesforce always strives to notify customers as quickly as possible once a service-impacting event has been detected.
- Part of that detection involves investigating the overall scope of the impact as well as determining which customers are affected by the incident.
- In some cases, the initial investigation may take some time to determine what the actual impact is and which customers are affected. When that happens, the Trust post can be delayed.
- At Salesforce, we try to strike the balance between rapidly acknowledging an

incident broadly and unnecessarily alerting customers to a situation that may not affect them.

Why weren't we made aware of your intent to fix the vulnerability before you made the change?

- As part of our standard remediation process, when we discover security vulnerabilities, we act immediately to close them. Pre-notification risks giving unauthorized third parties more time and awareness to exploit the vulnerability, which would put the safety of your data and your business at risk.

How did Salesforce respond?

- Salesforce is actively monitoring this issue and working to patch any Salesforce services that either use the vulnerable component, Log4j2, or provide it to customers.
- We also have threat detections in place to alert for exploitation attempts.

What Salesforce products are vulnerable/affected?

- For the protection of your company and other customers that may not yet have installed the security patch for this issue, we are not sharing this information at this time.

Where can I get additional information?

We're committed to keeping our customers informed. You can find the latest updates at <https://status.salesforce.com>.

As our internal FAQ is updated I will share any relevant details.

As always, any questions please dont hesitate to ask.

Thanks,

s47F - personal privacy

Customer Success Director | Salesforce - Canberra, Australia

Mobile: s47F - personal privacy | Email: s47F - personal privacy

Follow us on:    



From: §47F - personal privacy
To: §22(1)(a)(ii) - irrelevant material
Subject: ACTION REQUIRED: MuleSoft Security Update
Date: Thursday, 16 December 2021 1:01:09 AM

MuleSoft Header



MuleSoft is aware of the recently disclosed Apache Log4j2 vulnerability (CVE-2021-44228).

Please review the Knowledge Article, [Apache Log4j2 vulnerability - December 2021](#), for instructions on any actions you may need to take. We will post updates to the Knowledge Article as additional information becomes available.

We appreciate your trust in us as we continue to make your success our top priority.

Thank you,
MuleSoft

Salesforce.com, Inc. Salesforce Tower @ 415 Mission Street, 3rd Floor, San Francisco, CA, 94105, United States. General Enquiries: 415-901-7000

This email was sent to §22(1)(a)(ii) - irrelevant material
[Privacy Statement](#)

From: §47F - personal privacy
To: §22(1)(a)(ii) - irrelevant mate
Subject: ACTION REQUIRED: MuleSoft Security Update
Date: Thursday, 16 December 2021 1:02:11 AM

MuleSoft Header



MuleSoft is aware of the recently disclosed Apache Log4j2 vulnerability (CVE-2021-44228).

Please review the Knowledge Article, [Apache Log4j2 vulnerability - December 2021](#), for instructions on any actions you may need to take. We will post updates to the Knowledge Article as additional information becomes available.

We appreciate your trust in us as we continue to make your success our top priority.

Thank you,
MuleSoft

Salesforce.com, Inc. Salesforce Tower @ 415 Mission Street, 3rd Floor, San Francisco, CA, 94105, United States. General Enquiries: 415-901-7000

This email was sent to §22(1)(a)(ii) - irrelevant material
Privacy Statement

From: §47F - personal privacy
To: §22(1)(a)(i) - irrelevant m
Subject: ACTION REQUIRED: MuleSoft Security Update
Date: Thursday, 16 December 2021 1:02:13 AM

MuleSoft Header



MuleSoft is aware of the recently disclosed Apache Log4j2 vulnerability (CVE-2021-44228).

Please review the Knowledge Article, [Apache Log4j2 vulnerability - December 2021](#), for instructions on any actions you may need to take. We will post updates to the Knowledge Article as additional information becomes available.

We appreciate your trust in us as we continue to make your success our top priority.

Thank you,
MuleSoft

Salesforce.com, Inc. Salesforce Tower @ 415 Mission Street, 3rd Floor, San Francisco, CA, 94105, United States. General Enquiries: 415-901-7000

This email was sent to §22(1)(a)(i) - irrelevant material
Privacy Statement

From: §47F - personal privacy
To: §22(1)(a)(i) - irrelevant
Subject: ACTION REQUIRED: MuleSoft Security Update
Date: Thursday, 16 December 2021 1:02:15 AM

MuleSoft Header



MuleSoft is aware of the recently disclosed Apache Log4j2 vulnerability (CVE-2021-44228).

Please review the Knowledge Article, [Apache Log4j2 vulnerability - December 2021](#), for instructions on any actions you may need to take. We will post updates to the Knowledge Article as additional information becomes available.

We appreciate your trust in us as we continue to make your success our top priority.

Thank you,
MuleSoft

Salesforce.com, Inc. Salesforce Tower @ 415 Mission Street, 3rd Floor, San Francisco, CA, 94105, United States. General Enquiries: 415-901-7000

This email was sent to §22(1)(a)(i) - irrelevant material
Privacy Statement

From: s47F - personal privacy
To: s22(1)(a)(ii) - irrelevant material
Subject: ACTION REQUIRED: MuleSoft Security Update
Date: Thursday, 16 December 2021 1:02:25 AM

MuleSoft Header



MuleSoft is aware of the recently disclosed Apache Log4j2 vulnerability (CVE-2021-44228).

Please review the Knowledge Article, [Apache Log4j2 vulnerability - December 2021](#), for instructions on any actions you may need to take. We will post updates to the Knowledge Article as additional information becomes available.

We appreciate your trust in us as we continue to make your success our top priority.

Thank you,
MuleSoft

Salesforce.com, Inc. Salesforce Tower @ 415 Mission Street, 3rd Floor, San Francisco, CA, 94105, United States. General Enquiries: 415-901-7000

This email was sent to s22(1)(a)(ii) - irrelevant material
[Privacy Statement](#)