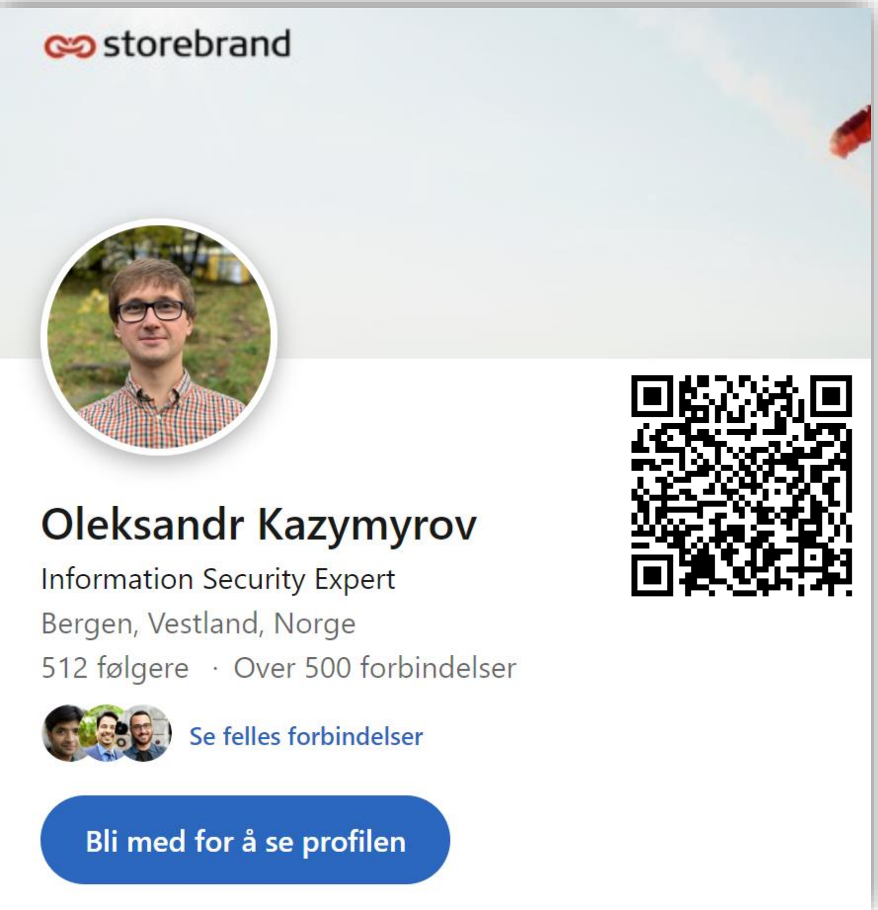
storebrand

What We’ve Learned from Exposing Atlassian on the Internet: In-Depth Analysis from an Offensive Perspective

Oleksandr Kazymyrov

BSides Munich 2023

Who am I?



storebrand

Oleksandr Kazymyrov

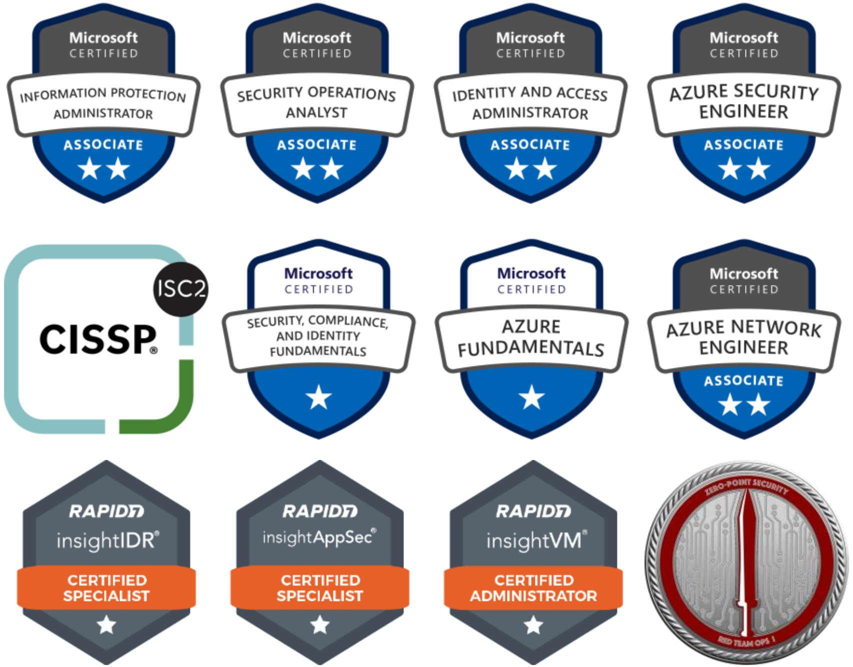
Information Security Expert

Bergen, Vestland, Norge

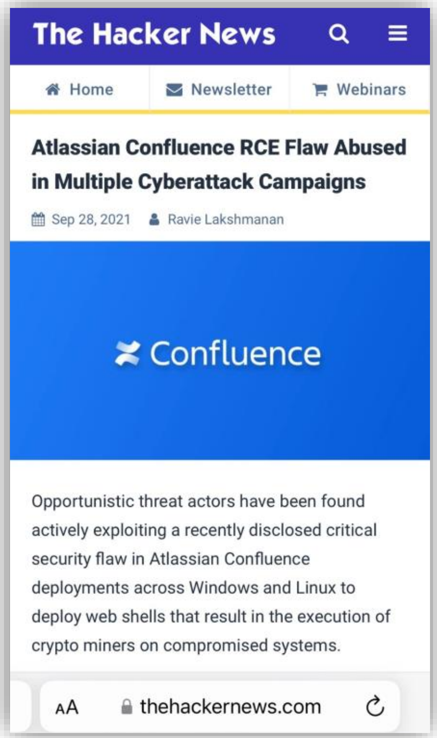
512 følgere · Over 500 forbindelser

Se felles forbindelser

Bli med for å se profilen



Atlassian in security news

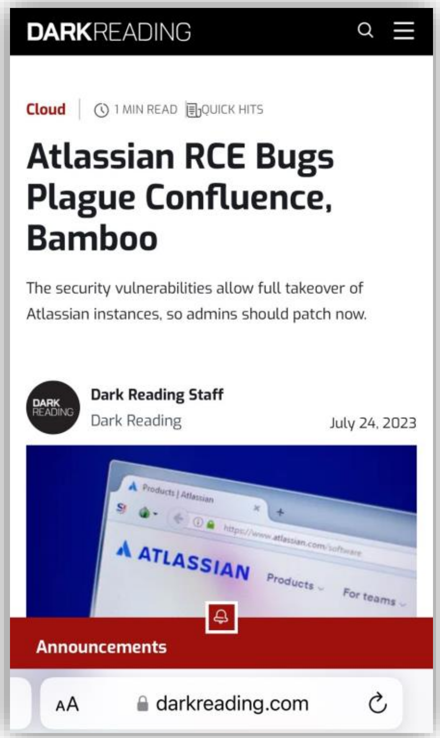

The Hacker News

Home | Newsletter | Webinars

Atlassian Confluence RCE Flaw Abused in Multiple Cyberattack Campaigns

Sep 28, 2021 · Ravie Lakshmanan

Opportunistic threat actors have been found actively exploiting a recently disclosed critical security flaw in Atlassian Confluence deployments across Windows and Linux to deploy web shells that result in the execution of crypto miners on compromised systems.

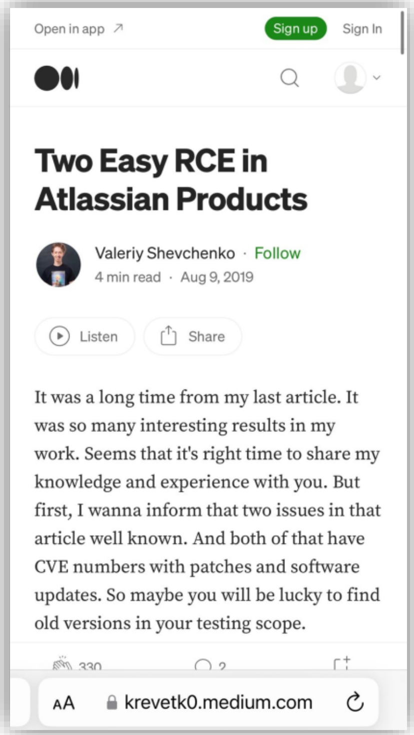

DARKREADING

Cloud | 1 MIN READ | QUICK HITS

Atlassian RCE Bugs Plague Confluence, Bamboo

The security vulnerabilities allow full takeover of Atlassian instances, so admins should patch now.

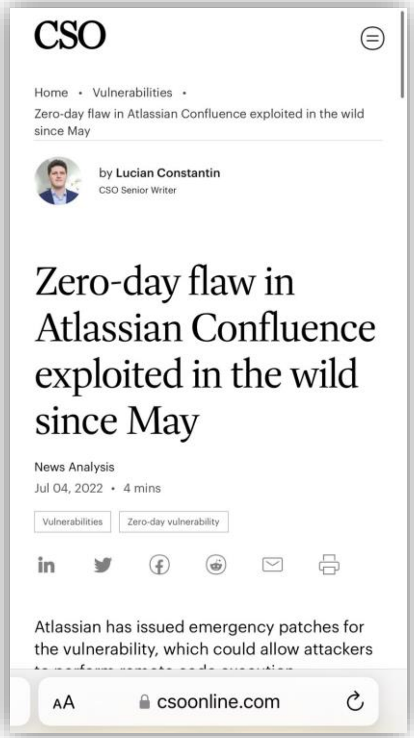
Dark Reading Staff
Dark Reading
July 24, 2023



Two Easy RCE in Atlassian Products

Valeriy Shevchenko · Follow
4 min read · Aug 9, 2019

It was a long time from my last article. It was so many interesting results in my work. Seems that it's right time to share my knowledge and experience with you. But first, I wanna inform that two issues in that article well known. And both of that have CVE numbers with patches and software updates. So maybe you will be lucky to find old versions in your testing scope.


CSO

Home • Vulnerabilities •
Zero-day flaw in Atlassian Confluence exploited in the wild since May

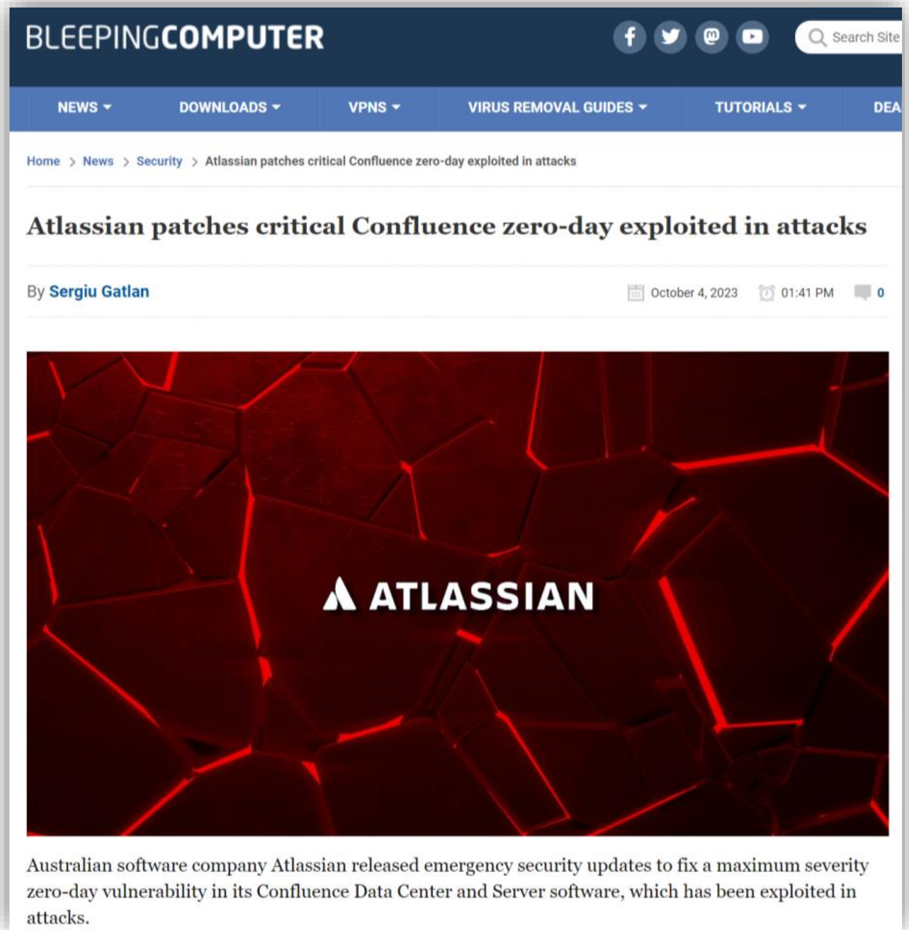
by Lucian Constantin
CSO Senior Writer

Zero-day flaw in Atlassian Confluence exploited in the wild since May

News Analysis
Jul 04, 2022 • 4 mins

Atlassian has issued emergency patches for the vulnerability, which could allow attackers

Atlassian in security news

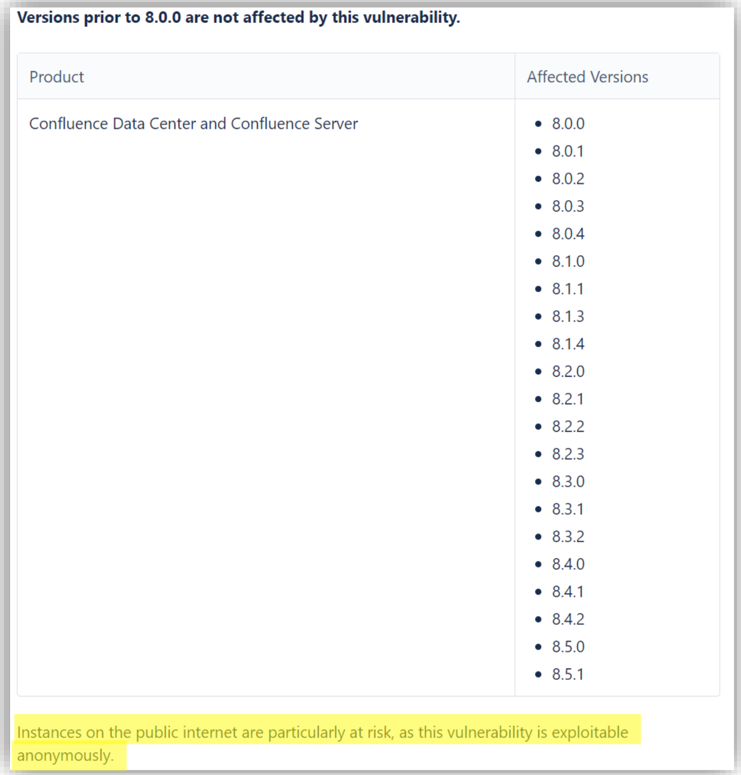


Home > News > Security > Atlassian patches critical Confluence zero-day exploited in attacks

Atlassian patches critical Confluence zero-day exploited in attacks

By Sergiu Gatlan October 4, 2023 01:41 PM 0

Australian software company Atlassian released emergency security updates to fix a maximum severity zero-day vulnerability in its Confluence Data Center and Server software, which has been exploited in attacks.

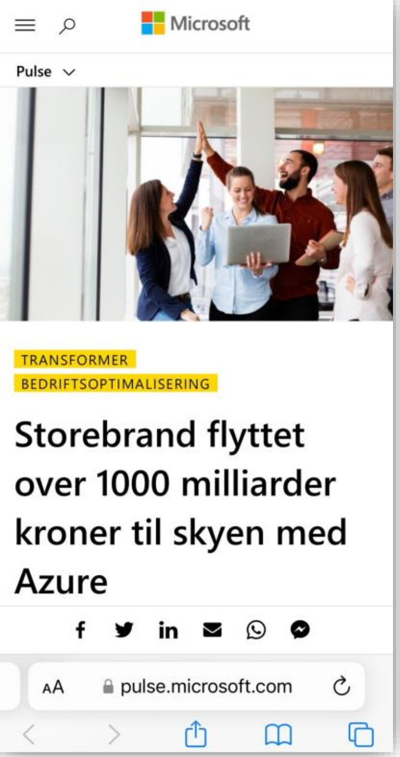


Versions prior to 8.0.0 are not affected by this vulnerability.

Product	Affected Versions
Confluence Data Center and Confluence Server	• 8.0.0 • 8.0.1 • 8.0.2 • 8.0.3 • 8.0.4 • 8.1.0 • 8.1.1 • 8.1.3 • 8.1.4 • 8.2.0 • 8.2.1 • 8.2.2 • 8.2.3 • 8.3.0 • 8.3.1 • 8.3.2 • 8.4.0 • 8.4.1 • 8.4.2 • 8.5.0 • 8.5.1

Instances on the public internet are particularly at risk, as this vulnerability is exploitable anonymously.

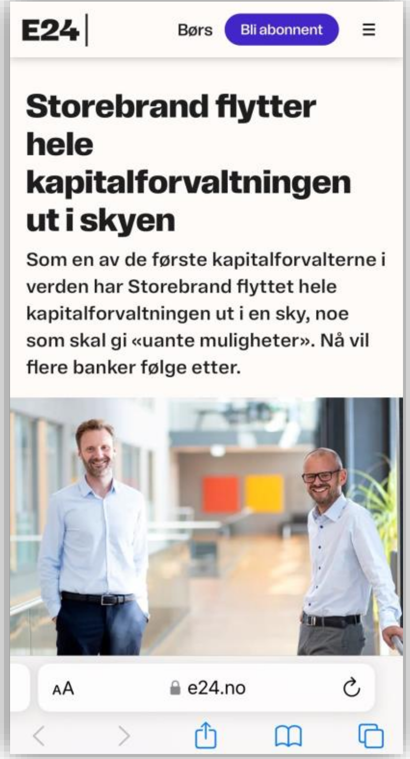
Storebrand in the cloud



TRANSFORMER

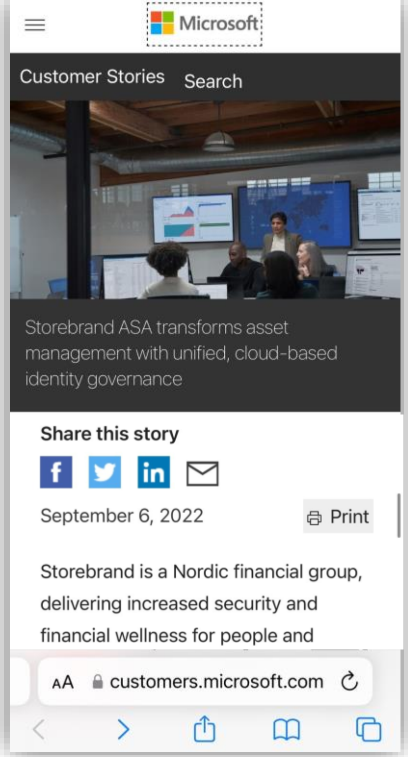
BEDRIFTSOPTIMALISERING

Storebrand flyttet over 1000 milliarder kroner til skyen med Azure



Storebrand flytter hele kapitalforvaltningen ut i skyen

Som en av de første kapitalforvalterne i verden har Storebrand flyttet hele kapitalforvaltningen ut i en sky, noe som skal gi «uante muligheter». Nå vil flere banker følge etter.

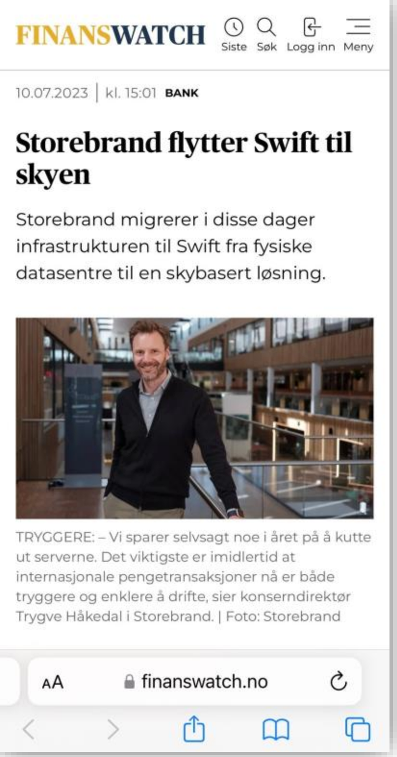


Storebrand ASA transforms asset management with unified, cloud-based identity governance

Share this story

September 6, 2022

Storebrand is a Nordic financial group, delivering increased security and financial wellness for people and



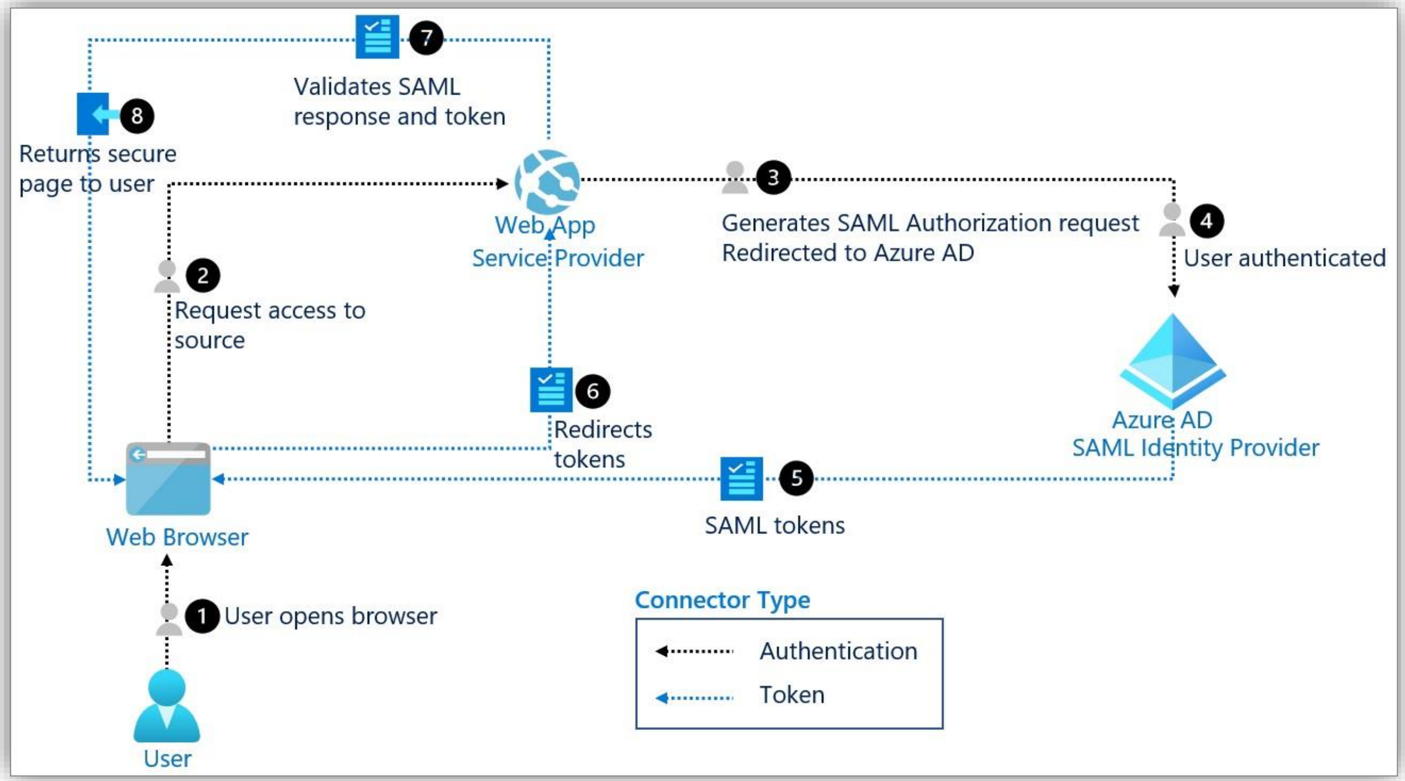
10.07.2023 | kl. 15:01 BANK

Storebrand flytter Swift til skyen

Storebrand migrerer i disse dager infrastrukturen til Swift fra fysiske datasentre til en skybasert løsning.

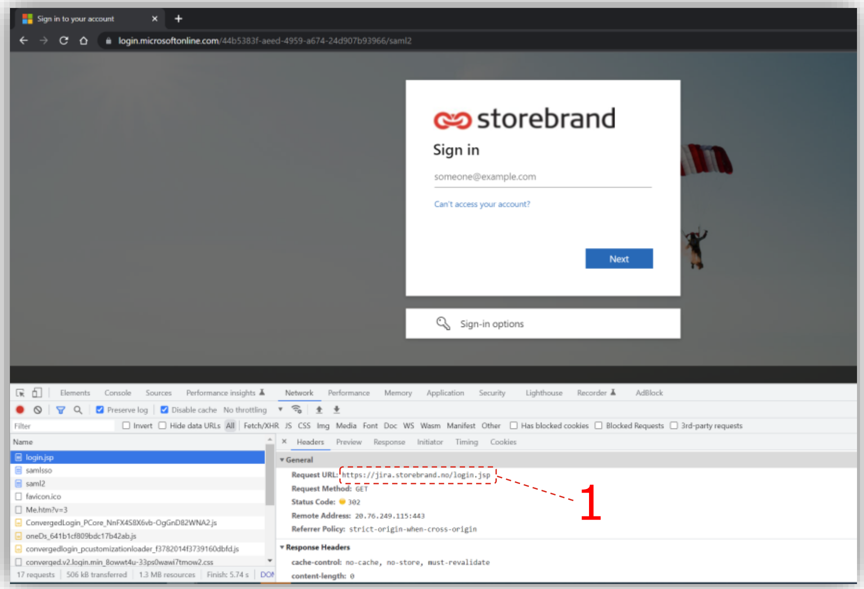
TRYGGERE: – Vi sparer selvsagt noe i året på å kutte ut serverne. Det viktigste er imidlertid at internasjonale pengetransaksjoner nå er både tryggere og enklere å drifte, sier konserndirektør Trygve Håkedal i Storebrand. | Foto: Storebrand

SAML authentication with Microsoft Entra ID

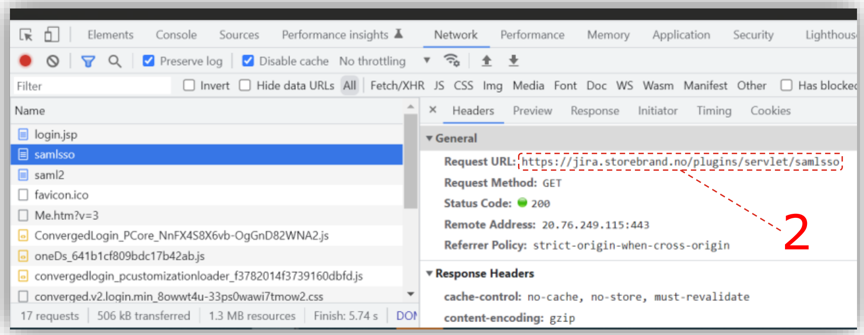


Source: SAML authentication with Microsoft Entra ID

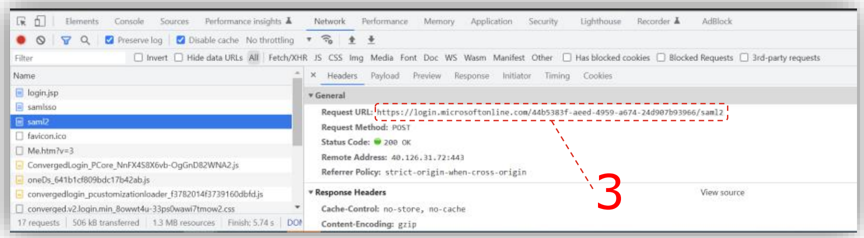
Azure AD: first steps in the authentication flow


Sign in to your account
login.microsoftonline.com/44b5383f-aeed-4959-a674-24d907b93966/saml2
storebrand
Sign in
someone@example.com
Can't access your account?
Next
Sign-in options
Elements Console Sources Performance insights Network Performance Memory Application Security Lighthouse Recorder AdBlock
☑ Preserve log ☑ Disable cache No throttling
Filter □ Invert □ Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other □ Has blocked cookies □ Blocked Requests □ 3rd-party requests
Headers Preview Response Initiator Timing Cookies
1

```
Name
login.jsp
samlsso
saml2
favicon.ico
Me.htm?v=3
ConvergedLogin_PCore_NnFX4S8X6vb-OgGnD82WNA2.js
oneDs_641b1cf809bdc17b42ab.js
convergedlogin_pcustomizationloader_f3782014f3739160dbfd.js
converged.v2.login.min_8owwt4u-33ps0wawi7tmow2.css
17 requests | 506 kB transferred | 1.3 MB resources | Finish: 5.74 s | DOM

▾ General
Request URL: https://jira.storebrand.no/login.jsp
Request Method: GET
Status Code: 302
Remote Address: 20.76.249.115:443
Referrer Policy: strict-origin-when-cross-origin
▾ Response Headers
cache-control: no-cache, no-store, must-revalidate
content-length: 0
```

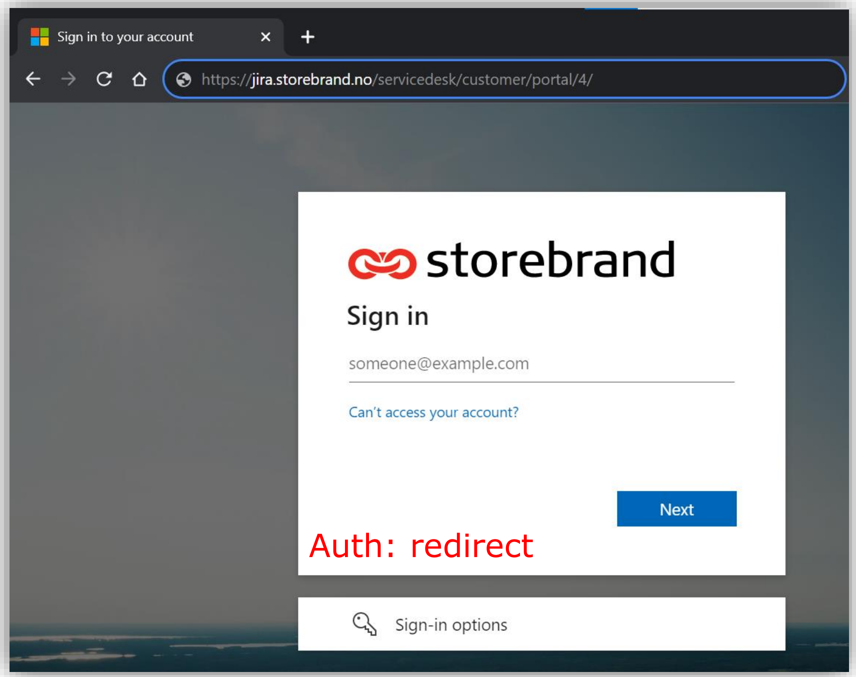

Elements Console Sources Performance insights Network Performance Memory Application Security Lighthous
☑ Preserve log ☑ Disable cache No throttling
Filter □ Invert □ Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other □ Has blocke
Headers Preview Response Initiator Timing Cookies
2

```
Name
login.jsp
samlsso
saml2
favicon.ico
Me.htm?v=3
ConvergedLogin_PCore_NnFX4S8X6vb-OgGnD82WNA2.js
oneDs_641b1cf809bdc17b42ab.js
convergedlogin_pcustomizationloader_f3782014f3739160dbfd.js
converged.v2.login.min_8owwt4u-33ps0wawi7tmow2.css
17 requests | 506 kB transferred | 1.3 MB resources | Finish: 5.74 s | DOM

▾ General
Request URL: https://jira.storebrand.no/plugins/servlet/samlsso
Request Method: GET
Status Code: 200
Remote Address: 20.76.249.115:443
Referrer Policy: strict-origin-when-cross-origin
▾ Response Headers
cache-control: no-cache, no-store, must-revalidate
content-encoding: gzip
```


Elements Console Sources Performance insights Network Performance Memory Application Security Lighthouse Recorder AdBlock
☑ Preserve log ☑ Disable cache No throttling
Filter □ Invert □ Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other □ Has blocked cookies □ Blocked Requests □ 3rd-party requests
Headers Payload Preview Response Initiator Timing Cookies
View source
3

```
Name
login.jsp
samlsso
saml2
favicon.ico
Me.htm?v=3
ConvergedLogin_PCore_NnFX4S8X6vb-OgGnD82WNA2.js
oneDs_641b1cf809bdc17b42ab.js
convergedlogin_pcustomizationloader_f3782014f3739160dbfd.js
converged.v2.login.min_8owwt4u-33ps0wawi7tmow2.css
17 requests | 506 kB transferred | 1.3 MB resources | Finish: 5.74 s | DOM

▾ General
Request URL: https://login.microsoftonline.com/44b5383f-aeed-4959-a674-24d907b93966/saml2
Request Method: POST
Status Code: 200 OK
Remote Address: 40.126.31.72:443
Referrer Policy: strict-origin-when-cross-origin
▾ Response Headers
Cache-Control: no-store, no-cache
Content-Encoding: gzip
```

SSO and WAF: expected behavior



https://jira.storebrand.no/servicedesk/customer/portal/4/

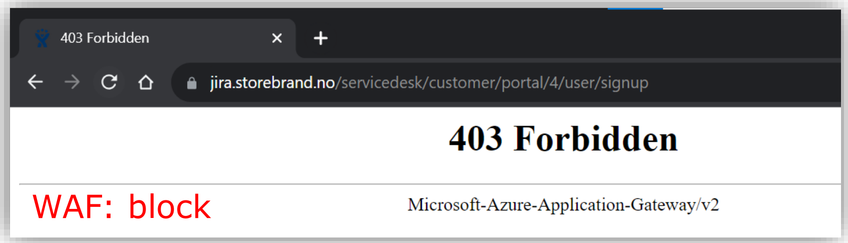
storebrand

Sign in

someone@example.com

Can't access your account?

Auth: redirect

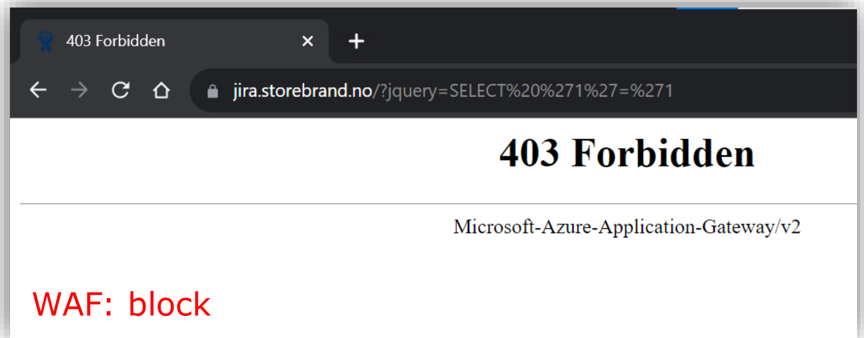


jira.storebrand.no/servicedesk/customer/portal/4/user/signup

403 Forbidden

Microsoft-Azure-Application-Gateway/v2

WAF: block



jira.storebrand.no/?jquery=SELECT%20%271%27=%271

403 Forbidden

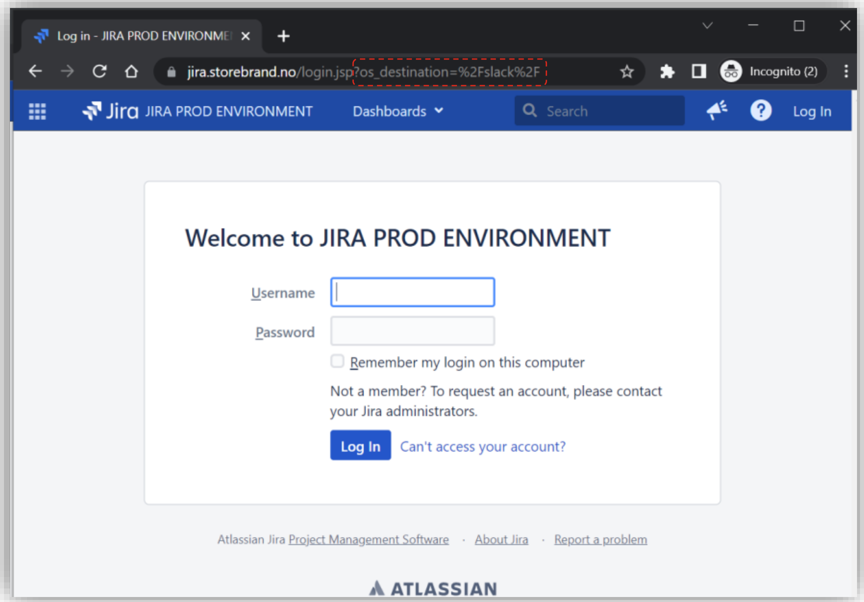
Microsoft-Azure-Application-Gateway/v2

WAF: block

Bypass SSO

This is URL to bypass SSO: https://jira-t.storebrand.no/login.jsp?os_destination=%2Fslack%2F

The most important part is **?os_destination=%2Fslack%2F**, which triggers Non SSO URLs



Log in - JIRA PROD ENVIRONME

jira.storebrand.no/login.jsp?os_destination=%2Fslack%2F

Incognito (2)

Jira JIRA PROD ENVIRONMENT Dashboards Search Log In

Welcome to JIRA PROD ENVIRONMENT

Username

Password

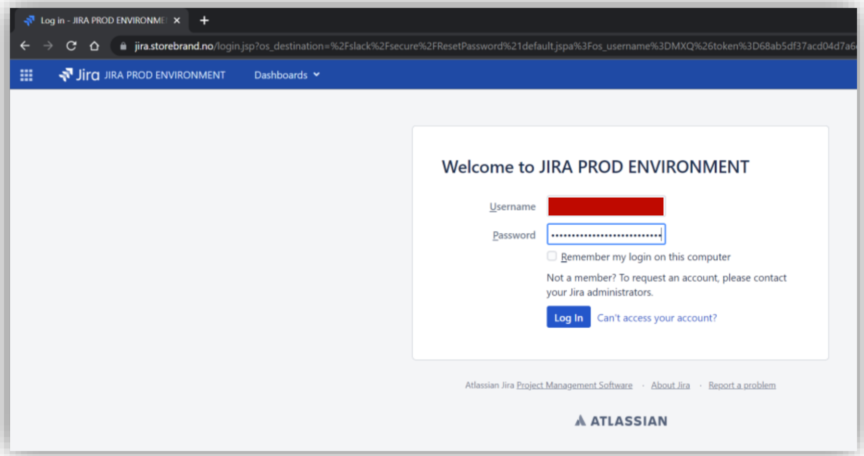
□ Remember my login on this computer

Not a member? To request an account, please contact your Jira administrators.

Log In Can't access your account?

Atlassian Jira Project Management Software · About Jira · Report a problem

ATLASSIAN



Log in - JIRA PROD ENVIRONME

jira.storebrand.no/login.jsp?os_destination=%2Fslack%2Fsecure%2FResetPassword%21default.jspa%3Fos_username%3DMXQ%26token%3D68ab5df37acd04d7a6

Jira JIRA PROD ENVIRONMENT Dashboards

Welcome to JIRA PROD ENVIRONMENT

Username [redacted]

Password ••••••••••••••••••••••••••••

□ Remember my login on this computer

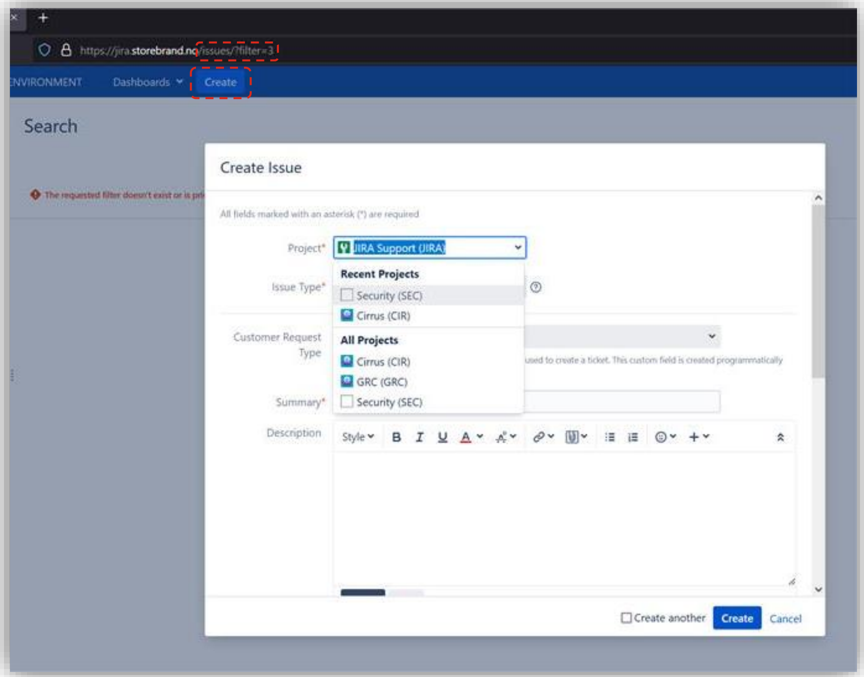
Not a member? To request an account, please contact your Jira administrators.

Log In Can't access your account?

Atlassian Jira Project Management Software · About Jira · Report a problem

ATLASSIAN

Anonymous access: information gathering over the Internet



https://jira.storebrand.no/issues/?filter=3

The requested filter doesn't exist or is pri

Create Issue

All fields marked with an asterisk (*) are required

Project*: JIRA Support (JIRA)

Recent Projects
- Security (SEC)
- Cirrus (CIR)

All Projects
- Cirrus (CIR)
- GRC (GRC)
- Security (SEC)

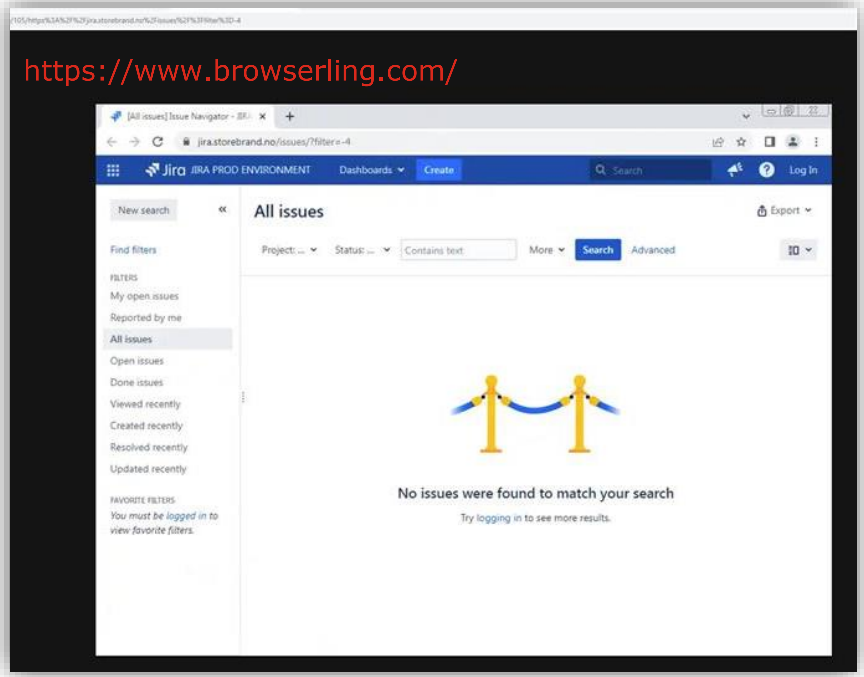
Issue Type*

Customer Request Type

used to create a ticket. This custom field is created programmatically

Summary*

Description



https://www.browserling.com/

[All issues] Issue Navigator - JIR

jira.storebrand.no/issues/?filter=-4

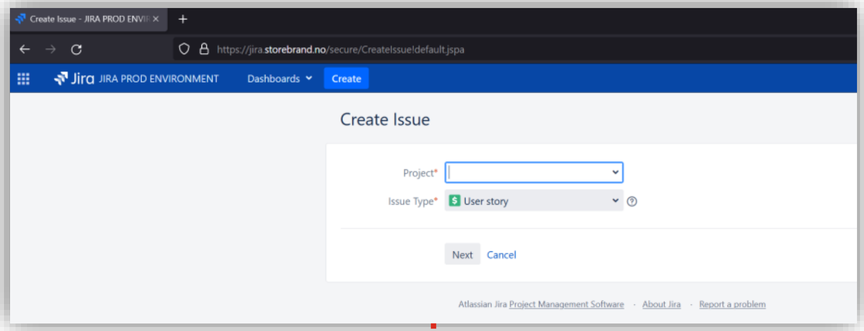
All issues

You must be logged in to view favorite filters.

No issues were found to match your search

Try logging in to see more results.

Anonymous access: create an issue

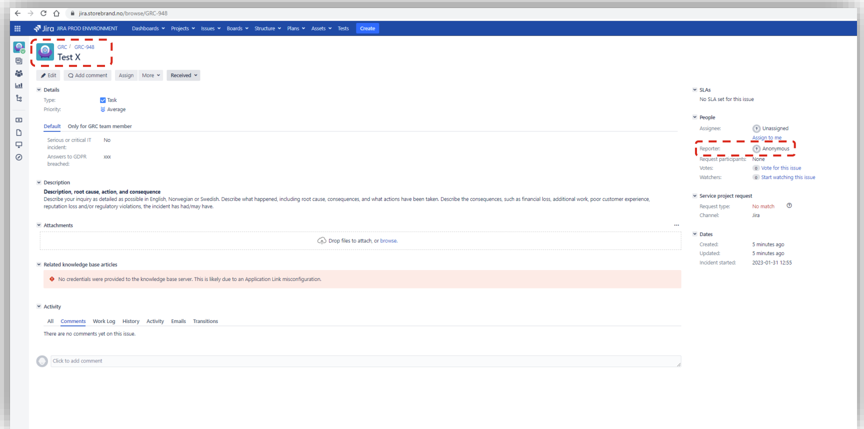

Create Issue - JIRA PROD ENVI
https://jira.storebrand.no/secure/CreateIssue!default.jspa
Jira JIRA PROD ENVIRONMENT
Dashboards
Create
Next
Cancel

Create Issue

Project*

Issue Type* User story

Atlassian Jira Project Management Software · About Jira · Report a problem



GRC / GRC-948

Test X

Details

Type: Task

Priority: Average

Default Only for GRC team member

Serious or critical IT incident: No

Answers to GDPR breached: xxx

Description

Description, root cause, action, and consequence

Describe your inquiry as detailed as possible in English, Norwegian or Swedish. Describe what happened, including root cause, consequences, and what actions have been taken. Describe the consequences, such as financial loss, additional work, poor customer experience, reputation loss and/or regulatory violations, the incident has had/may have.

Attachments

Drop files to attach, or browse.

Related knowledge base articles

No credentials were provided to the knowledge base server. This is likely due to an Application Link misconfiguration.

Activity

All Comments Work Log History Activity Emails Transitions

There are no comments yet on this issue.

Click to add comment

SLAs

No SLA set for this issue

People

Assignee: Unassigned

Assign to me

Reporter: Anonymous

Request participants: None

Votes: 0 Vote for this issue

Watchers: 0 Start watching this issue

Service project request

Request type: No match

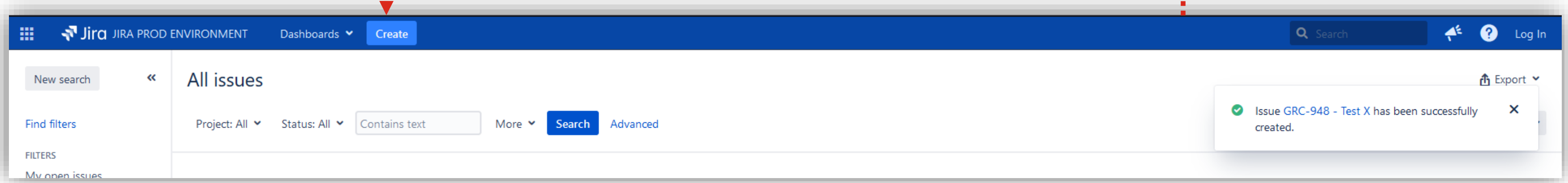
Channel: Jira

Dates

Created: 5 minutes ago

Updated: 5 minutes ago

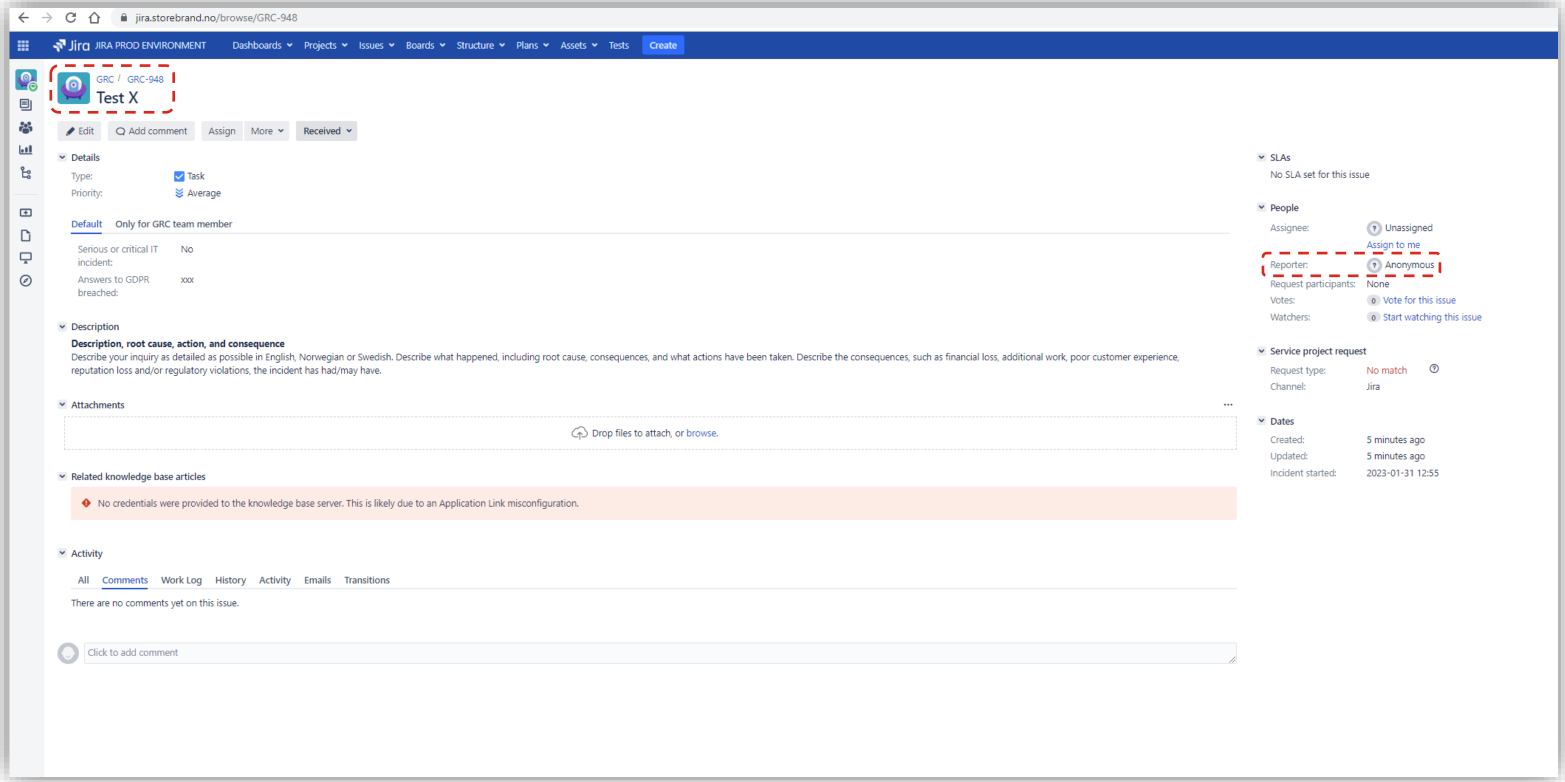
Incident started: 2023-01-31 12:55



All issues

Issue GRC-948 - Test X has been successfully created.

Anonymous access: create an issue



GRC / GRC-948

Test X

Details

Type: Task

Priority: Average

Default | Only for GRC team member

Serious or critical IT incident: No

Answers to GDPR breached: xxx

Description

Description, root cause, action, and consequence

Describe your inquiry as detailed as possible in English, Norwegian or Swedish. Describe what happened, including root cause, consequences, and what actions have been taken. Describe the consequences, such as financial loss, additional work, poor customer experience, reputation loss and/or regulatory violations, the incident has had/may have.

Attachments

Drop files to attach, or browse.

Related knowledge base articles

No credentials were provided to the knowledge base server. This is likely due to an Application Link misconfiguration.

Activity

All | Comments | Work Log | History | Activity | Emails | Transitions

There are no comments yet on this issue.

Click to add comment

SLAs

No SLA set for this issue

People

Assignee: Unassigned
Assign to me

Reporter: Anonymous

Request participants: None

Votes: 0 Vote for this issue

Watchers: 0 Start watching this issue

Service project request

Request type: No match

Channel: Jira

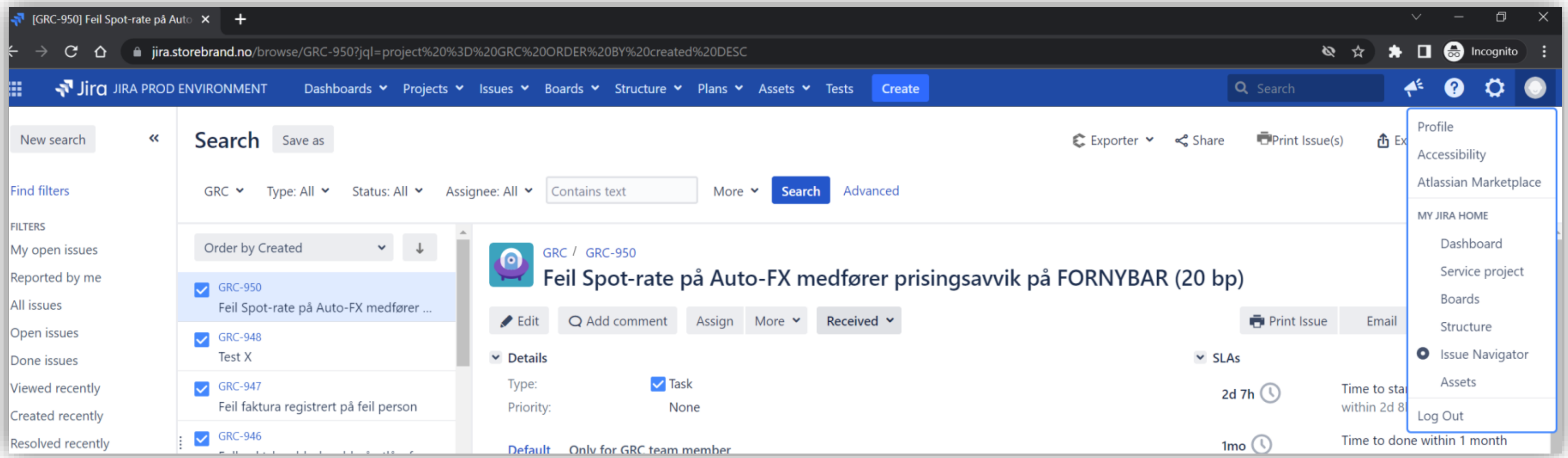
Dates

Created: 5 minutes ago

Updated: 5 minutes ago

Incident started: 2023-01-31 12:55

Anonymous access: search for low-hanging fruits



jira.storebrand.no/browse/GRC-950?jql=project%20%3D%20GRC%20ORDER%20BY%20created%20DESC

Search

GRC | Type: All | Status: All | Assignee: All | Contains text

Order by Created

- ☑ GRC-950 Feil Spot-rate på Auto-FX medfører ...
- ☑ GRC-948 Test X
- ☑ GRC-947 Feil faktura registrert på feil person
- ☑ GRC-946

GRC / GRC-950

Feil Spot-rate på Auto-FX medfører prisingsavvik på FORNYBAR (20 bp)

Details

Type: ☑ Task

Priority: None

Default Only for GRC team member

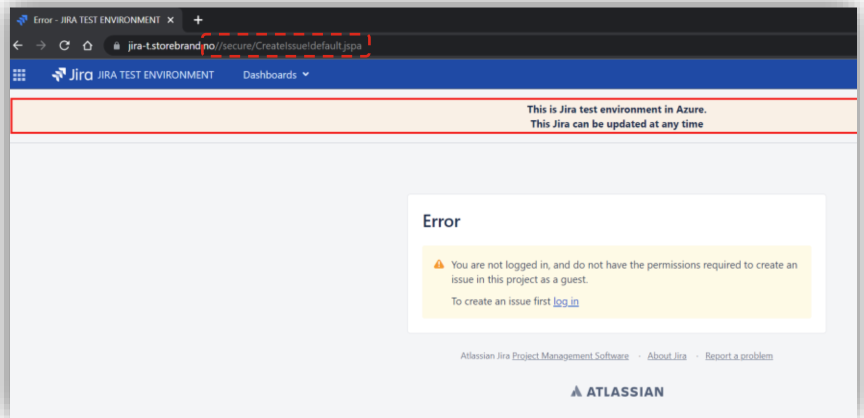
SLAs

2d 7h Time to sta… within 2d 8…

1mo Time to done within 1 month

storebrand

Impact: brute force


Error - JIRA TEST ENVIRONMENT
jira-t.storebrand.no//secure/CreateIssue!default.jspa
Jira JIRA TEST ENVIRONMENT
Dashboards

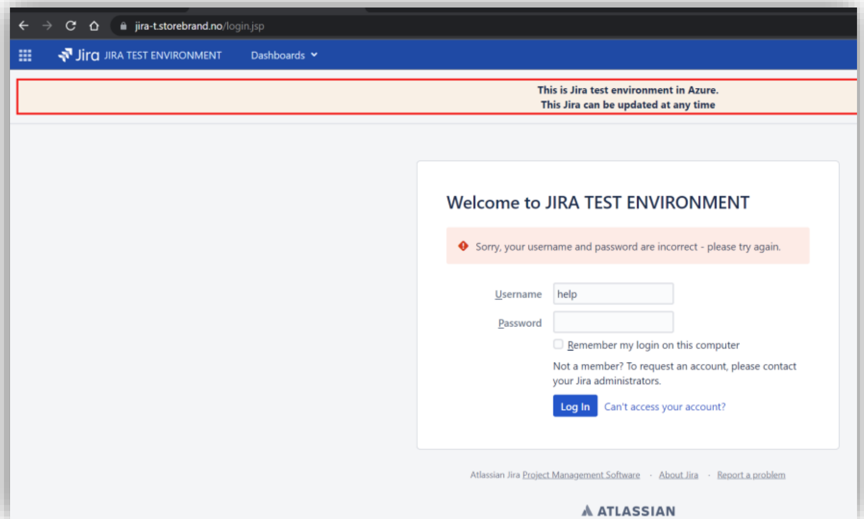
This is Jira test environment in Azure.
This Jira can be updated at any time

Error

You are not logged in, and do not have the permissions required to create an issue in this project as a guest.

To create an issue first log in

Atlassian Jira Project Management Software · About Jira · Report a problem
ATLASSIAN


jira-t.storebrand.no/login.jsp
Jira JIRA TEST ENVIRONMENT
Dashboards

This is Jira test environment in Azure.
This Jira can be updated at any time

Welcome to JIRA TEST ENVIRONMENT

Sorry, your username and password are incorrect - please try again.

Username: help

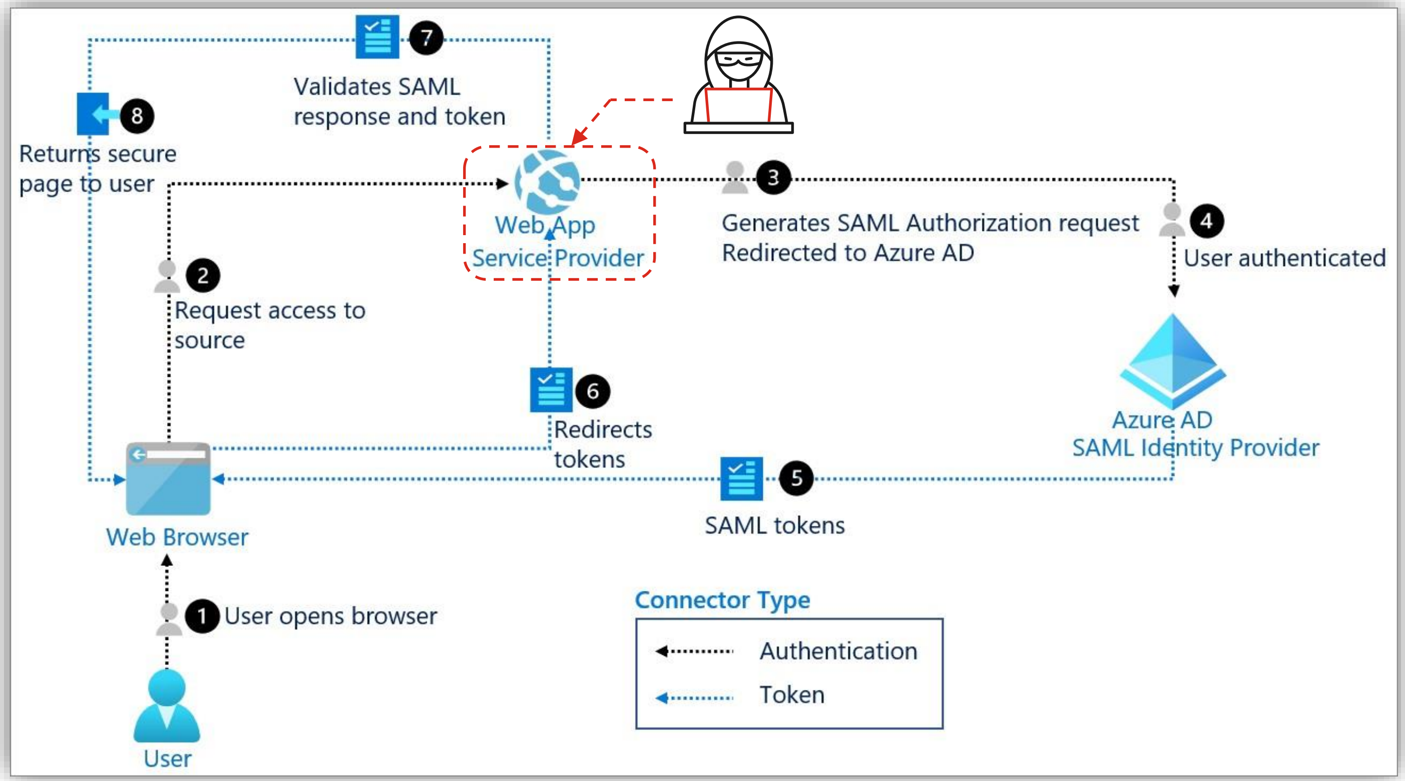
Password:

□ Remember my login on this computer

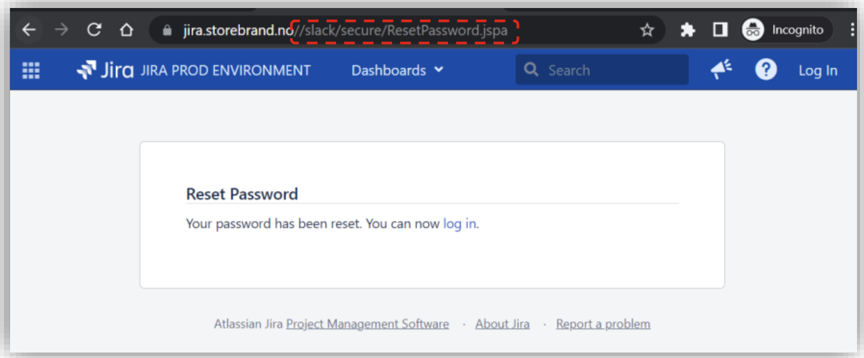
Not a member? To request an account, please contact your Jira administrators.

Log In
Can't access your account?
Atlassian Jira Project Management Software · About Jira · Report a problem
ATLASSIAN

SAML authentication with Microsoft Entra ID



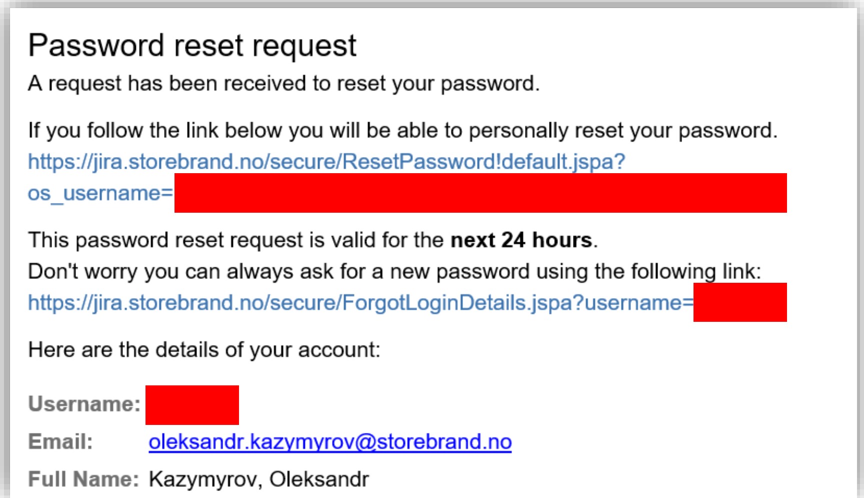
Impact: password reset (via Jira)


jira.storebrand.no//slack/secure/ResetPassword.jspa
Incognito
Jira JIRA PROD ENVIRONMENT
Dashboards
Search
Log In

Reset Password

Your password has been reset. You can now log in.

Atlassian Jira Project Management Software · About Jira · Report a problem



Password reset request

A request has been received to reset your password.

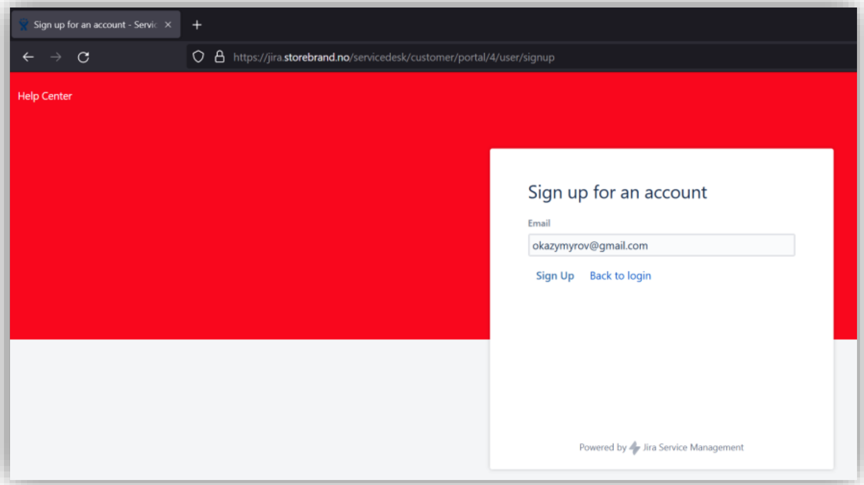
If you follow the link below you will be able to personally reset your password.
https://jira.storebrand.no/secure/ResetPassword!default.jspa?os_username=[redacted]

This password reset request is valid for the **next 24 hours**.
Don't worry you can always ask for a new password using the following link:
https://jira.storebrand.no/secure/ForgotLoginDetails.jspa?username=[redacted]

Here are the details of your account:

Username: [redacted]
Email: oleksandr.kazymyrov@storebrand.no
Full Name: Kazymyrov, Oleksandr

Impact: sign up for an account



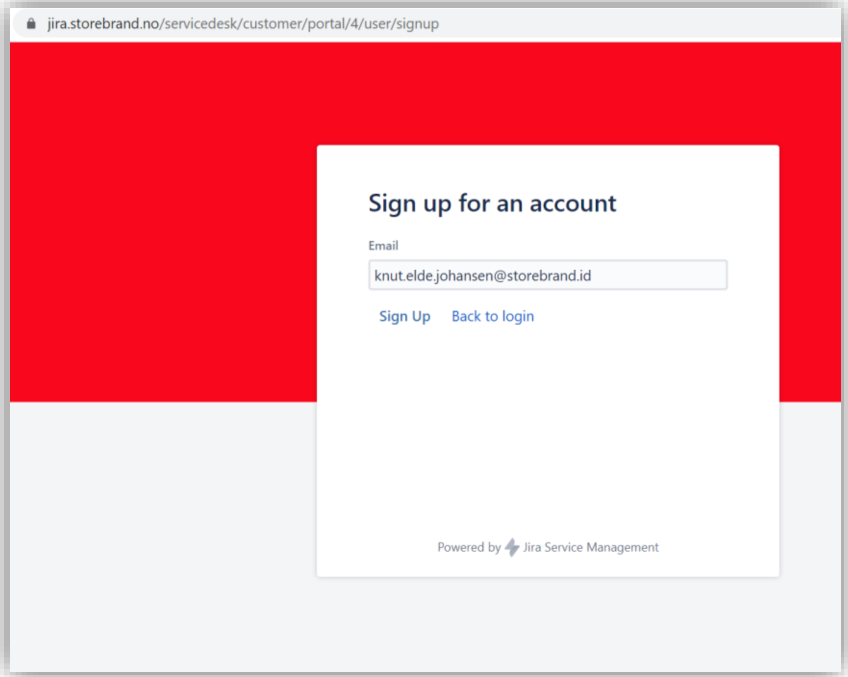
Sign up for an account - Servic
https://jira.storebrand.no/servicedesk/customer/portal/4/user/signup
Help Center

Sign up for an account

Email

okazymyrov@gmail.com

Sign Up
Back to login
Powered by Jira Service Management



jira.storebrand.no/servicedesk/customer/portal/4/user/signup

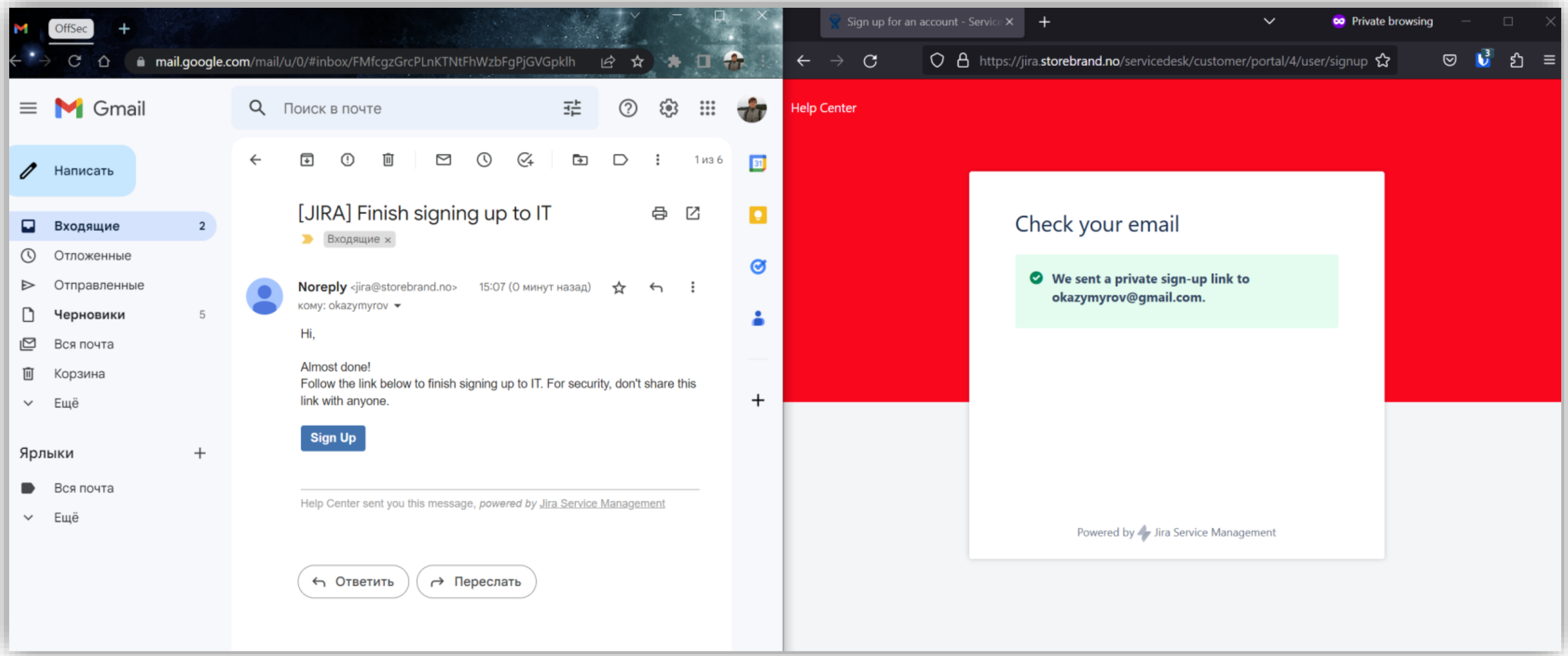
Sign up for an account

Email

knut.elde.johansen@storebrand.id

Sign Up
Back to login
Powered by Jira Service Management

Impact: sign up for an account



[JIRA] Finish signing up to IT

Noreply <jira@storebrand.no> 15:07 (0 минут назад)
кому: okazymyrov

Hi,

Almost done!
Follow the link below to finish signing up to IT. For security, don't share this link with anyone.

Sign Up

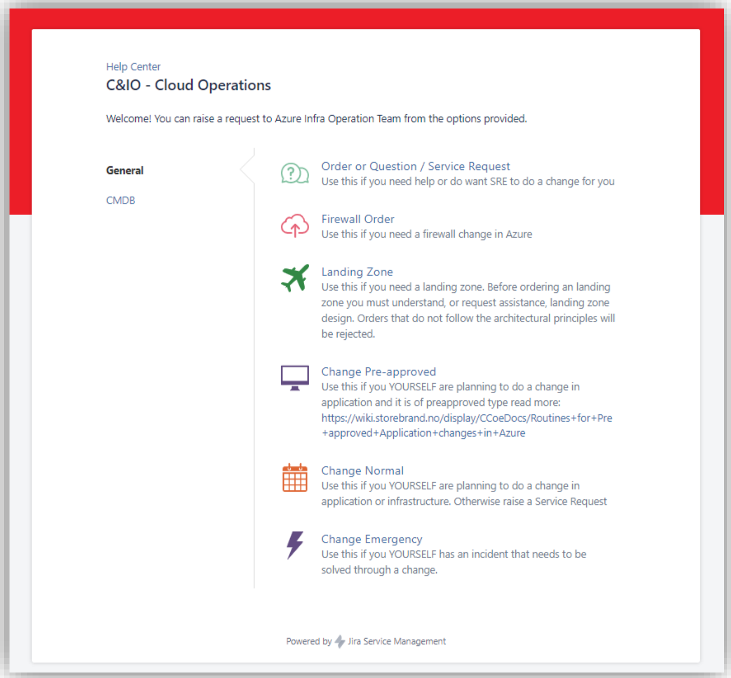
Help Center sent you this message, *powered by* Jira Service Management

Check your email

We sent a private sign-up link to okazymyrov@gmail.com.

Powered by Jira Service Management

Impact: enumeration / reconnaissance



Help Center

C&IO - Cloud Operations

Welcome! You can raise a request to Azure Infra Operation Team from the options provided.

General

CMDB

Order or Question / Service Request
Use this if you need help or do want SRE to do a change for you

Firewall Order
Use this if you need a firewall change in Azure

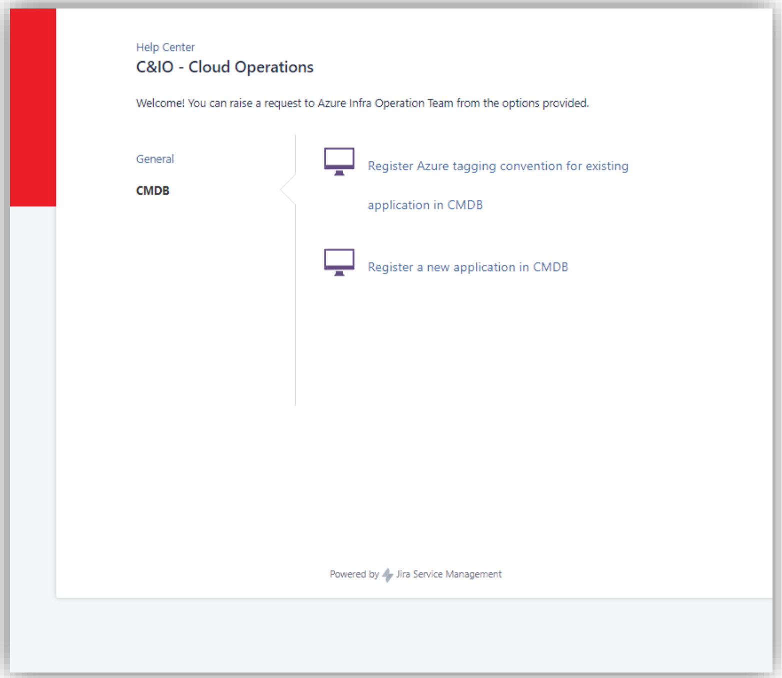
Landing Zone
Use this if you need a landing zone. Before ordering an landing zone you must understand, or request assistance, landing zone design. Orders that do not follow the architectural principles will be rejected.

Change Pre-approved
Use this if you YOURSELF are planning to do a change in application and it is of preapproved type read more: https://wiki.storebrand.no/display/CCoeDocs/Routines+for+Pre+approved+Application+changes+in+Azure

Change Normal
Use this if you YOURSELF are planning to do a change in application or infrastructure. Otherwise raise a Service Request

Change Emergency
Use this if you YOURSELF has an incident that needs to be solved through a change.

Powered by Jira Service Management



Help Center

C&IO - Cloud Operations

Welcome! You can raise a request to Azure Infra Operation Team from the options provided.

General

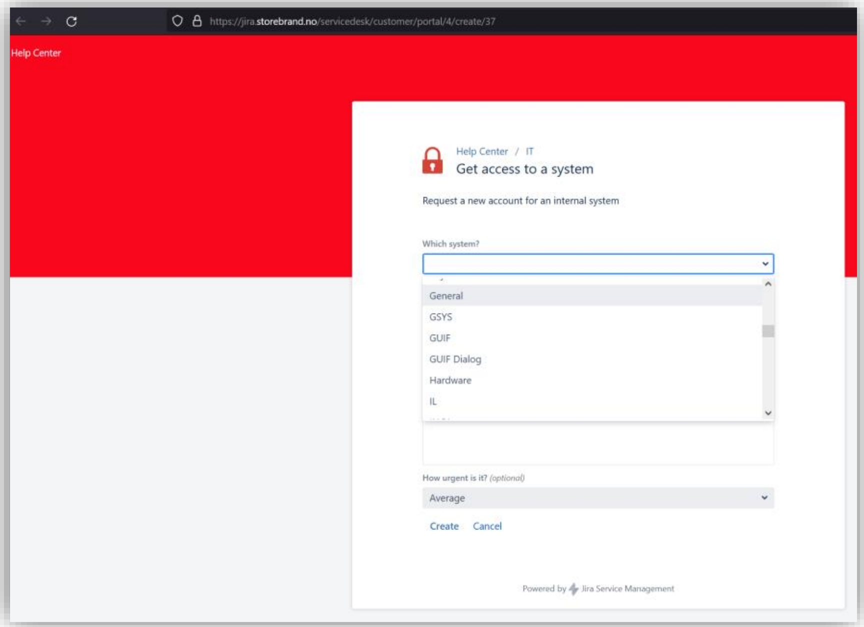
CMDB

Register Azure tagging convention for existing application in CMDB

Register a new application in CMDB

Powered by Jira Service Management

Impact: enumeration / reconnaissance



https://jira.storebrand.no/servicedesk/customer/portal/4/create/37

Help Center

Help Center / IT

Get access to a system

Request a new account for an internal system

Which system?

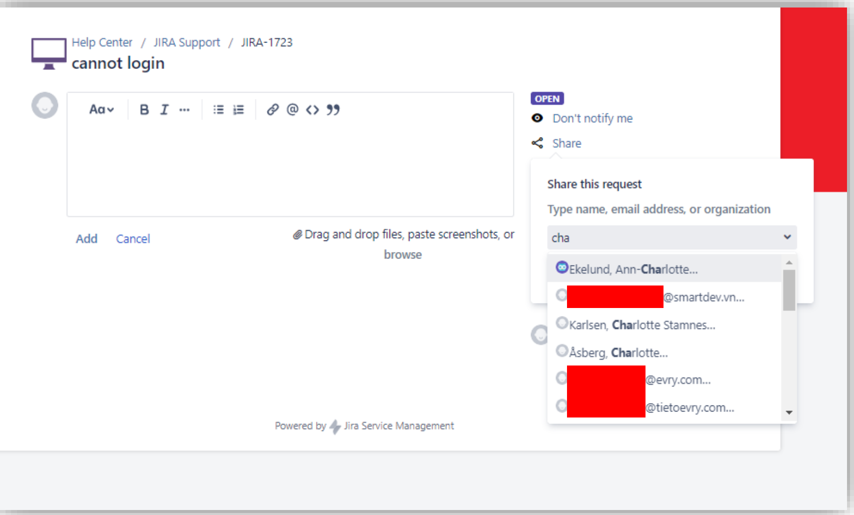
- General
- GSYS
- GUIF
- GUIF Dialog
- Hardware
- IL

How urgent is it? *(optional)*

Average

Create Cancel

Powered by Jira Service Management



Help Center / JIRA Support / JIRA-1723

cannot login

Add Cancel

Drag and drop files, paste screenshots, or browse

OPEN

Don't notify me

Share

Share this request

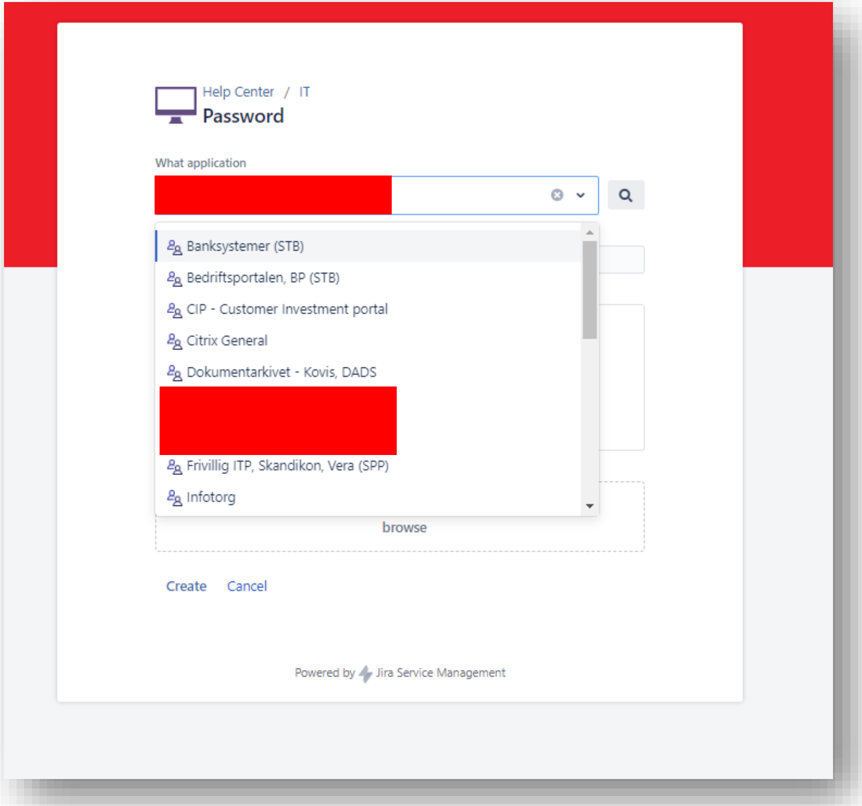
Type name, email address, or organization

cha

- Ekelund, Ann-**Cha**rlotte...
- [redacted]@smartdev.vn...
- Karlsen, **Cha**rlotte Stamnes...
- Åsberg, **Cha**rlotte...
- [redacted]@evry.com...
- @tietoevry.com...

Powered by Jira Service Management

Impact: social engineering via IT support



Help Center / IT

Password

What application

[redacted]

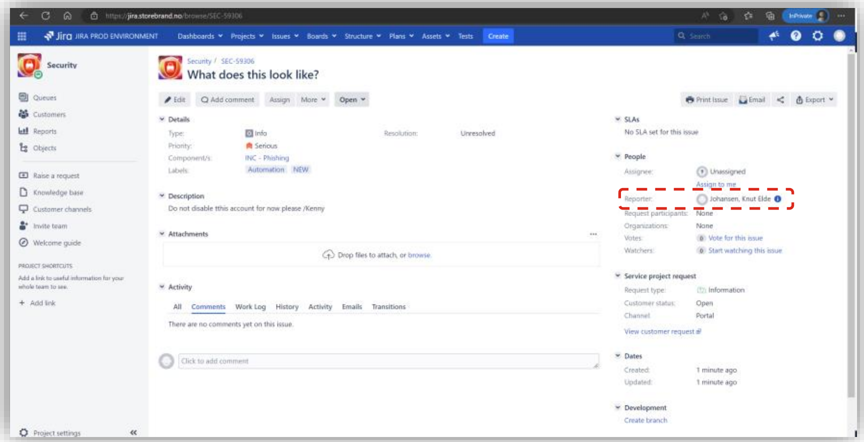
- Banksystemer (STB)
- Bedriftsportalen, BP (STB)
- CIP - Customer Investment portal
- Citrix General
- Dokumentarkivet - Kovis, DADS
- [redacted]
- Frivillig ITP, Skandikon, Vera (SPP)
- Infotorg

browse

Create Cancel

Powered by Jira Service Management

Impact: social engineering via IT support



Security / SEC-59306

What does this look like?

Details

Type: Info

Priority: Serious

Component/s: INC - Phishing

Labels: Automation NEW

Resolution: Unresolved

Description

Do not disable tthis account for now please /Kenny

Attachments

Activity

There are no comments yet on this issue.

SLAs

No SLA set for this issue

People

Assignee: Unassigned

Reporter: Johansen, Knut Elde

Request participants: None

Organizations: None

Votes: 0

Watchers: 0

Service project request

Request type: Information

Customer status: Open

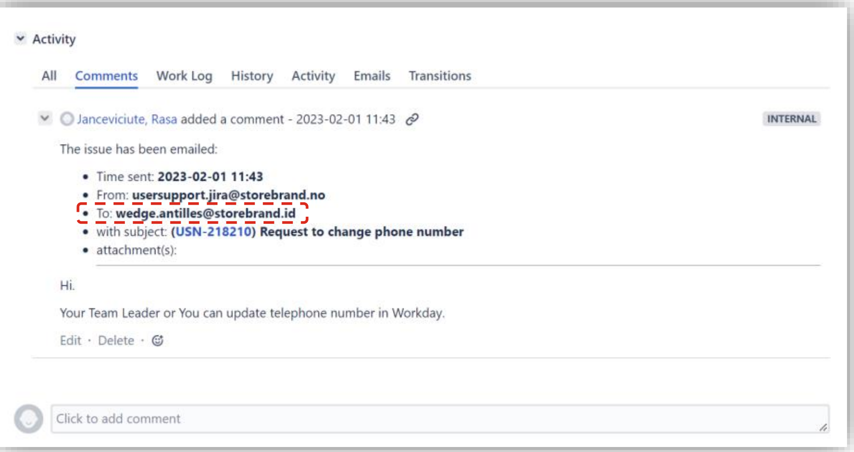
Channel: Portal

Dates

Created: 1 minute ago

Updated: 1 minute ago

Development



Janceviciute, Rasa added a comment - 2023-02-01 11:43

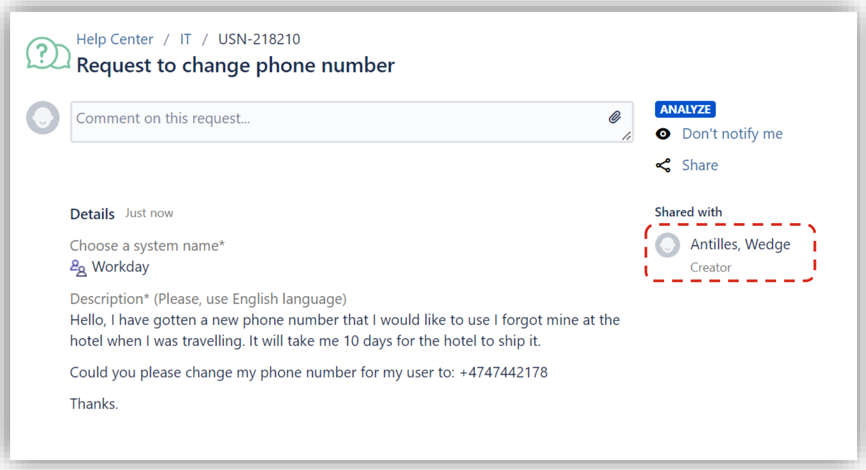
The issue has been emailed:

- Time sent: **2023-02-01 11:43**
- From: **usersupport.jira@storebrand.no**
- To: **wedge.antilles@storebrand.id**
- with subject: **(USN-218210) Request to change phone number**
- attachment(s):

Hi.

Your Team Leader or You can update telephone number in Workday.

Impact: social engineering via IT support



Help Center / IT / USN-218210

Request to change phone number

Comment on this request...

ANALYZE

Don't notify me

Share

Details Just now

Choose a system name*

Workday

Description* (Please, use English language)

Hello, I have gotten a new phone number that I would like to use I forgot mine at the hotel when I was travelling. It will take me 10 days for the hotel to ship it.

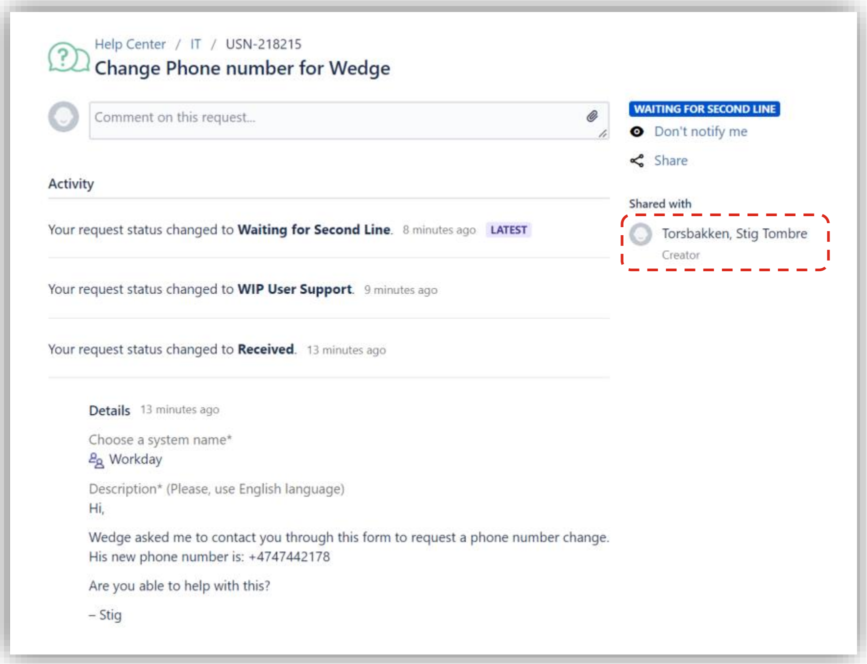
Could you please change my phone number for my user to: +4747442178

Thanks.

Shared with

Antilles, Wedge

Creator



Help Center / IT / USN-218215

Change Phone number for Wedge

Comment on this request...

WAITING FOR SECOND LINE

Don't notify me

Share

Activity

Your request status changed to **Waiting for Second Line**. 8 minutes ago LATEST

Your request status changed to **WIP User Support**. 9 minutes ago

Your request status changed to **Received**. 13 minutes ago

Details 13 minutes ago

Choose a system name*

Workday

Description* (Please, use English language)

Hi,

Wedge asked me to contact you through this form to request a phone number change. His new phone number is: +4747442178

Are you able to help with this?

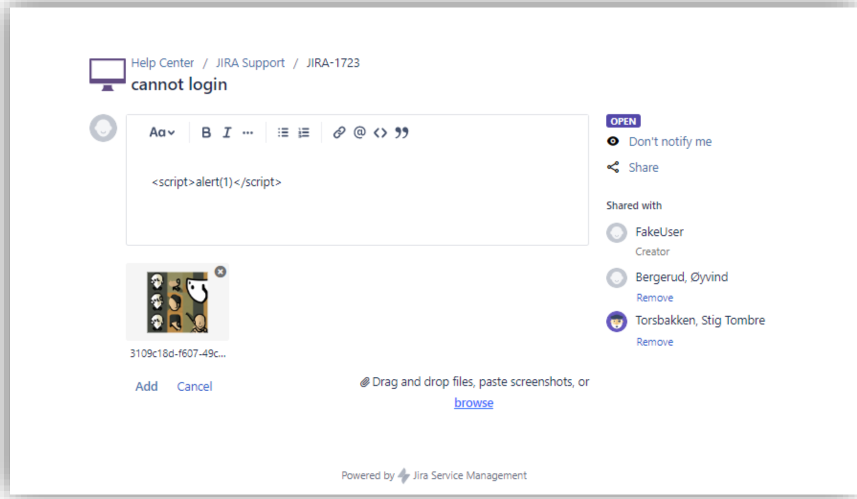
– Stig

Shared with

Torsbakken, Stig Tombre

Creator

Impact: social engineering via IT support



Help Center / JIRA Support / JIRA-1723

cannot login

```
<script>alert(1)</script>
```

3109c18d-f607-49c...

Drag and drop files, paste screenshots, or browse

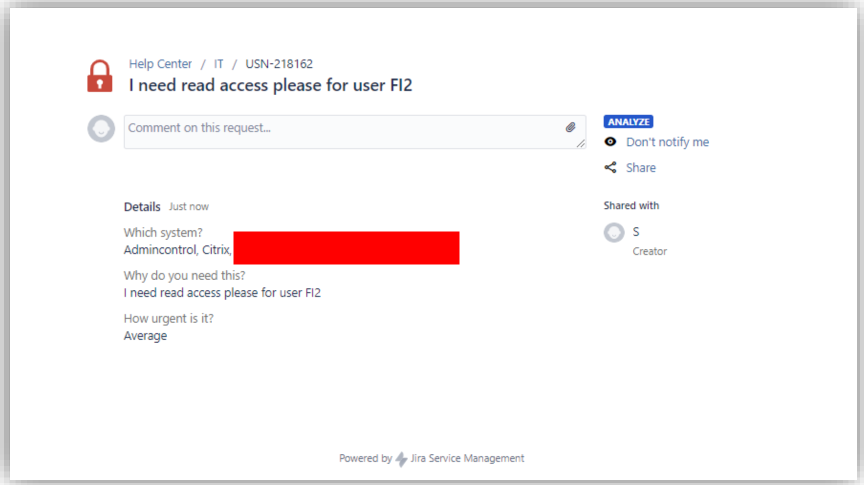
Shared with

FakeUser
Creator

Bergerud, Øyvind
Remove

Torsbakken, Stig Tombre
Remove

Powered by Jira Service Management



Help Center / IT / USN-218162

I need read access please for user FI2

Details Just now

Which system?
Admincontrol, Citrix, [redacted]

Why do you need this?
I need read access please for user FI2

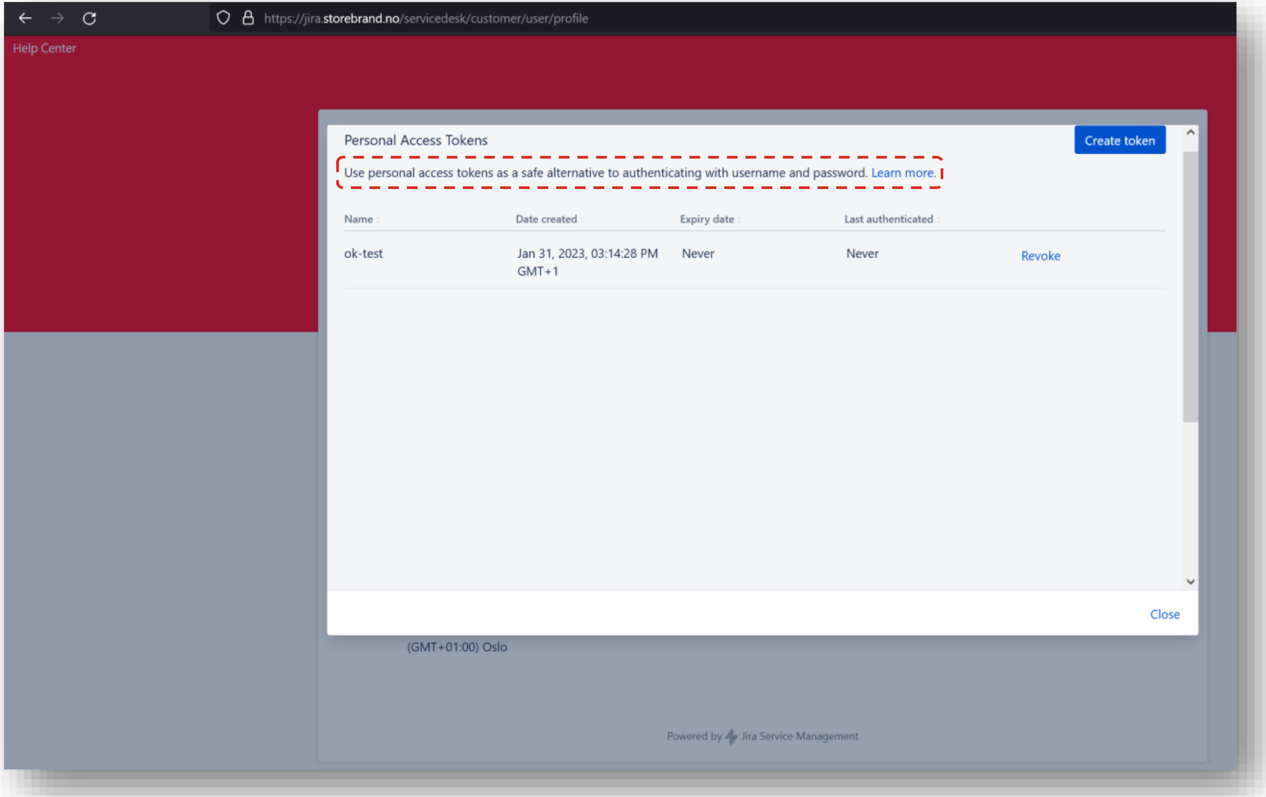
How urgent is it?
Average

Shared with

S
Creator

Powered by Jira Service Management

Impact: backdoor



https://jira.storebrand.no/servicedesk/customer/user/profile
Help Center

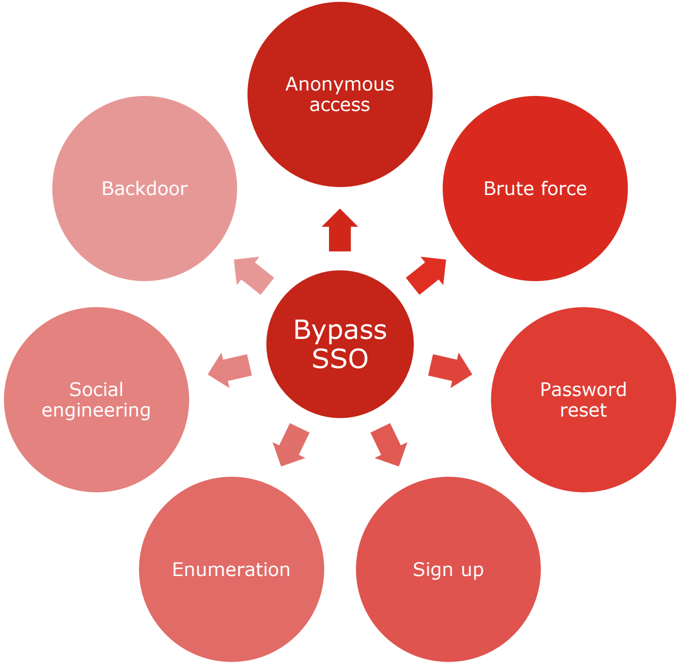
Personal Access Tokens

Use personal access tokens as a safe alternative to authenticating with username and password. Learn more.

Name	Date created	Expiry date	Last authenticated	
ok-test	Jan 31, 2023, 03:14:28 PM GMT+1	Never	Never	Revoke

Close
(GMT+01:00) Oslo
Powered by Jira Service Management

Summary of impact



Bypass SSO

Anonymous access

Brute force

Password reset

Sign up

Enumeration

Social engineering

Backdoor

”

Our greatest glory is not in never falling, but in rising every time we fall.

Confucius