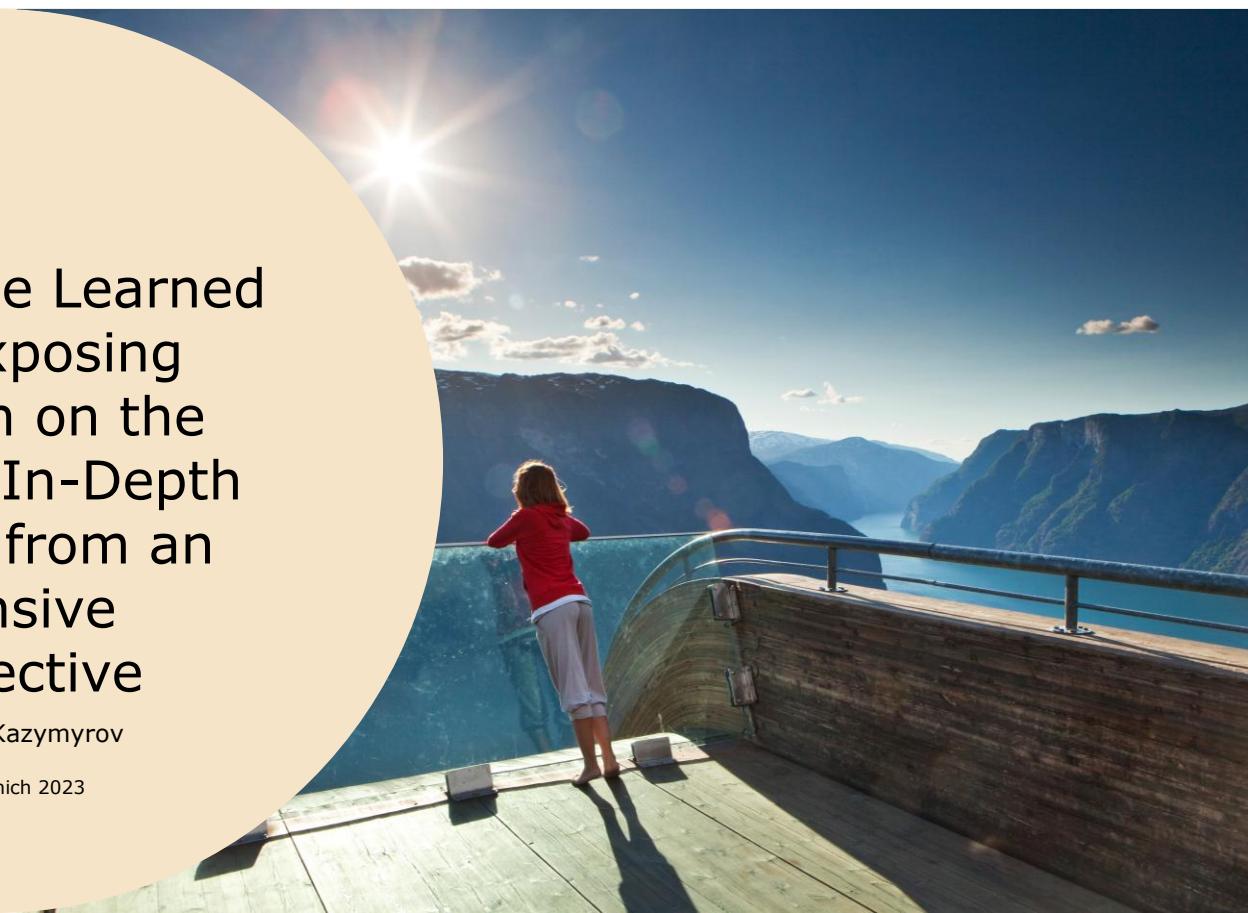


What We've Learned from Exposing Atlassian on the Internet: In-Depth Analysis from an Offensive Perspective

Oleksandr Kazymyrov

BSides Munich 2023





Oleksandr Kazymyrov

Information Security Expert

Bergen, Vestland, Norge

512 følgere · Over 500 forbindelser



Se felles forbindelser

Bli med for å se profilen



Who am I?



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.

AA  thehackernews.com 

DARKREADING  

Cloud | 1 MIN READ 

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



Announcements

[Open in app](#)  

Two Easy RCE in Atlassian Products

 Valeriy Shevchenko ·  4 min read · Aug 9, 2019

 Listen  Share

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.

AA  krevetk0.medium.com 

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

AA  csoonline.com 

[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.

Atlassian in security news

Versions prior to 8.0.0 are not affected by this vulnerability.

Product	Affected Versions
Confluence Data Center and Confluence Server	<ul style="list-style-type: none">8.0.08.0.18.0.28.0.38.0.48.1.08.1.18.1.38.1.48.2.08.2.18.2.28.2.38.3.08.3.18.3.28.4.08.4.18.4.28.5.08.5.1

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

Storebrand in the cloud



Microsoft

Pulse

TRANSFORMER
BEDRIFTSOPTIMALISERING

Storebrand flyttet over 1000 milliarder kroner til skyen med Azure

f      

AA pulse.microsoft.com 

< >   

Storebrand flyttet over 1000 milliarder kroner til skyen med Azure

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.



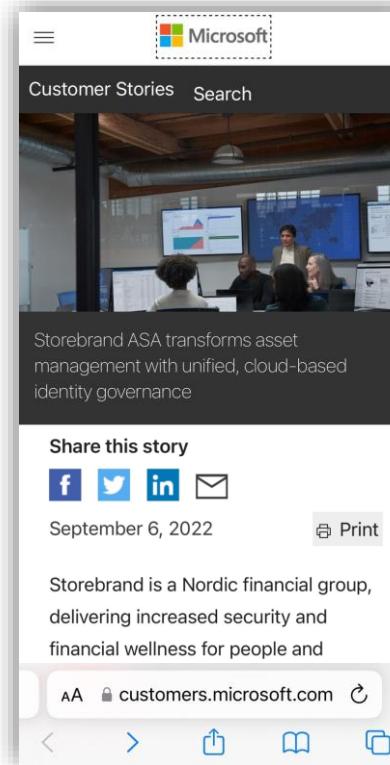


E24 | Børs  

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.





Microsoft

Customer Stories 

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

Share this story

f    

September 6, 2022 

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

AA customers.microsoft.com 

< >   



FINANSWATCH     

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.

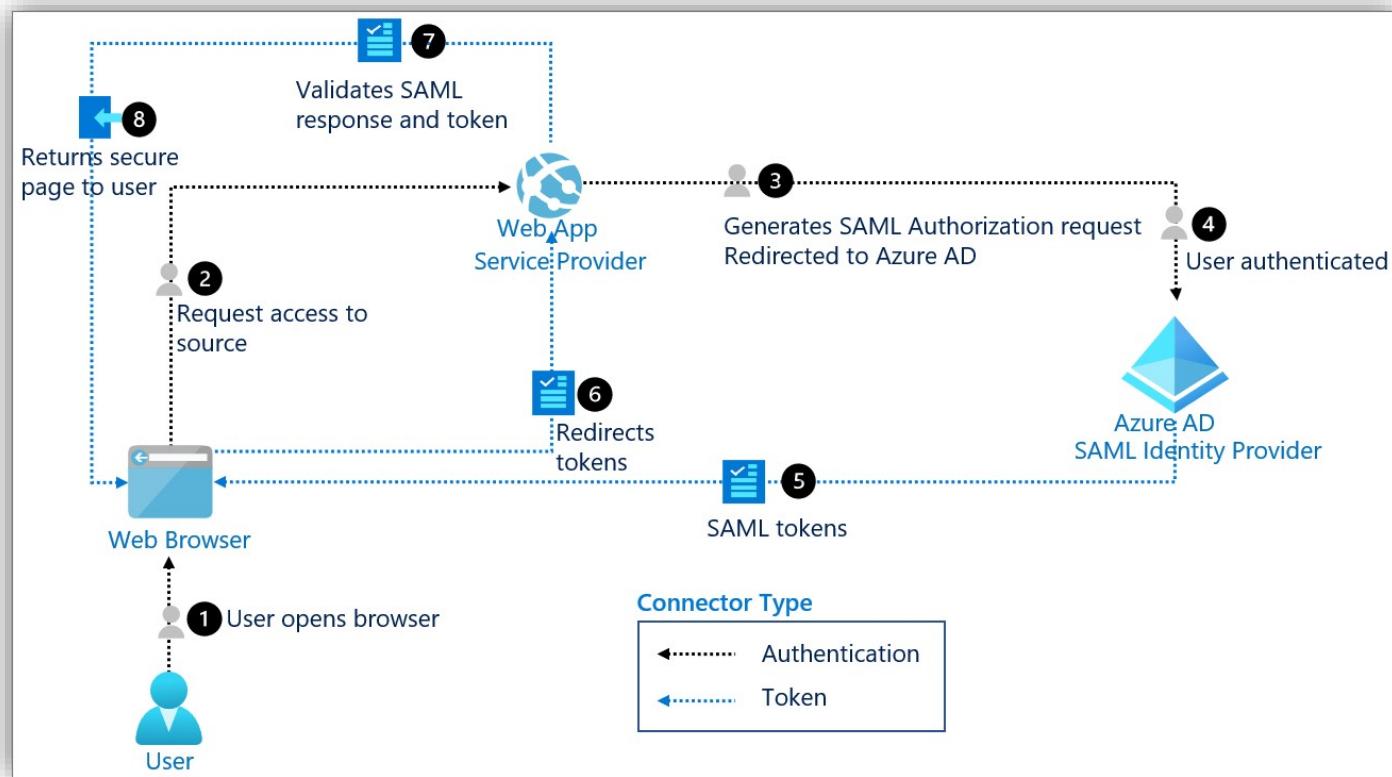


TRYGGERE: – Vi sparer selvagt noe i året på å kutte ut serverne. Det viktigste er imidlertid at internasjonale pengetransaksjoner nå er både tryggere og enklere å drifta, sier konserndirektør Trygve Håkedal i Storebrand. | Foto: Storebrand

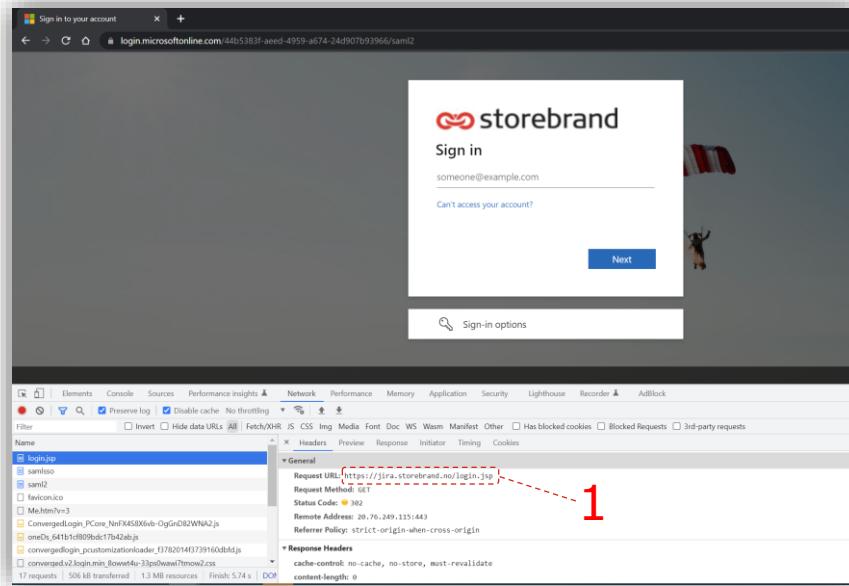
AA finanswatch.no 

< >   

SAML authentication with Microsoft Entra ID



Azure AD: first steps in the authentication flow



Sign in to your account

login.microsoftonline.com/44b538f1-aeed-4959-a674-24d907b93966/saml2

storebrand

Sign in

someone@example.com

Can't access your account?

Next

Sign-in options

Network

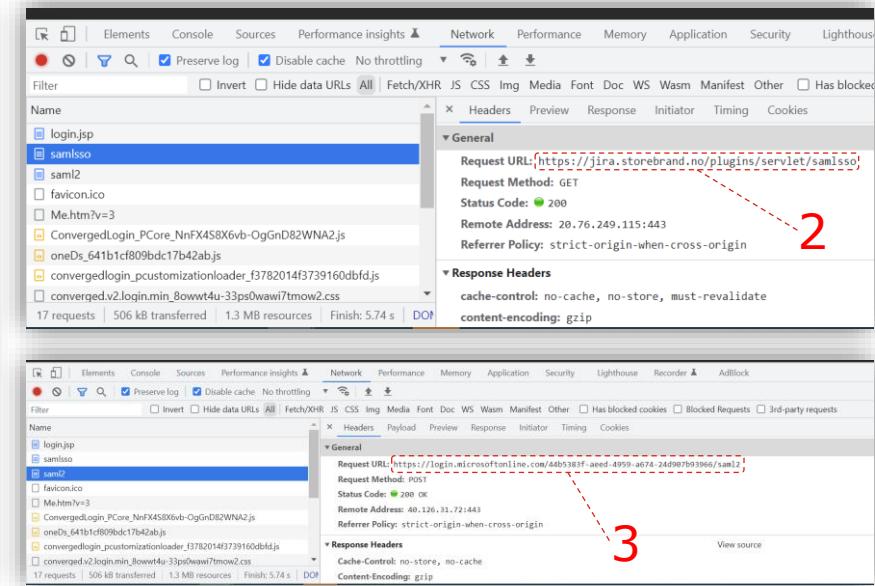
Request URL: https://jira.storebrand.no/plugins/servlet/samlso

Request Method: GET

Status Code: 200 OK

Remote Address: 20.76.249.115:443

Referrer Policy: strict-origin-when-cross-origin



Elements

Console

Sources

Performance insights

Network

Performance

Memory

Application

Security

Lighthouse

Headers

Preview

Response

Initiator

Timing

Cookies

General

Request URL: https://jira.storebrand.no/plugins/servlet/samlso

Request Method: GET

Status Code: 200 OK

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

General

Request URL: https://login.microsoftonline.com/44b538f1-aeed-4959-a674-24d907b93966/saml2

Request Method: POST

Status Code: 200 OK

Remote Address: 40.126.31.72:443

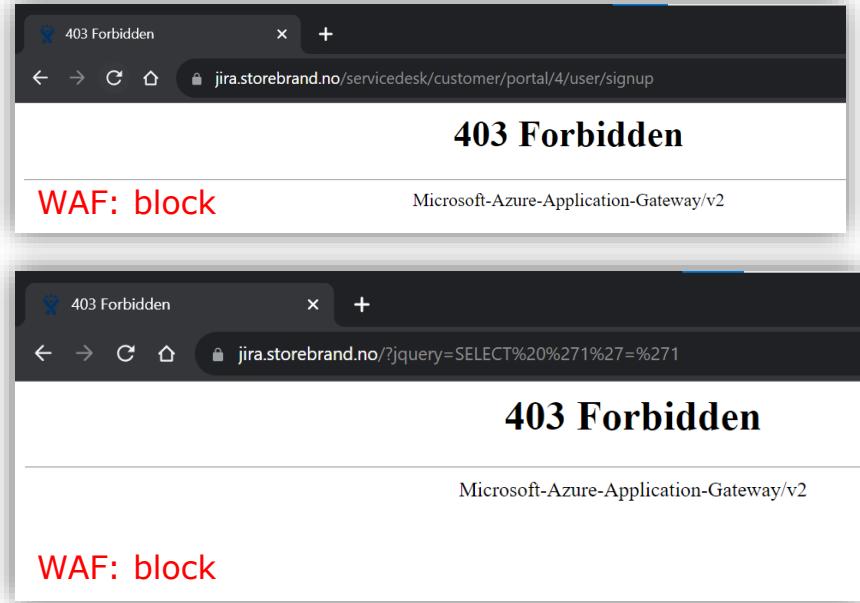
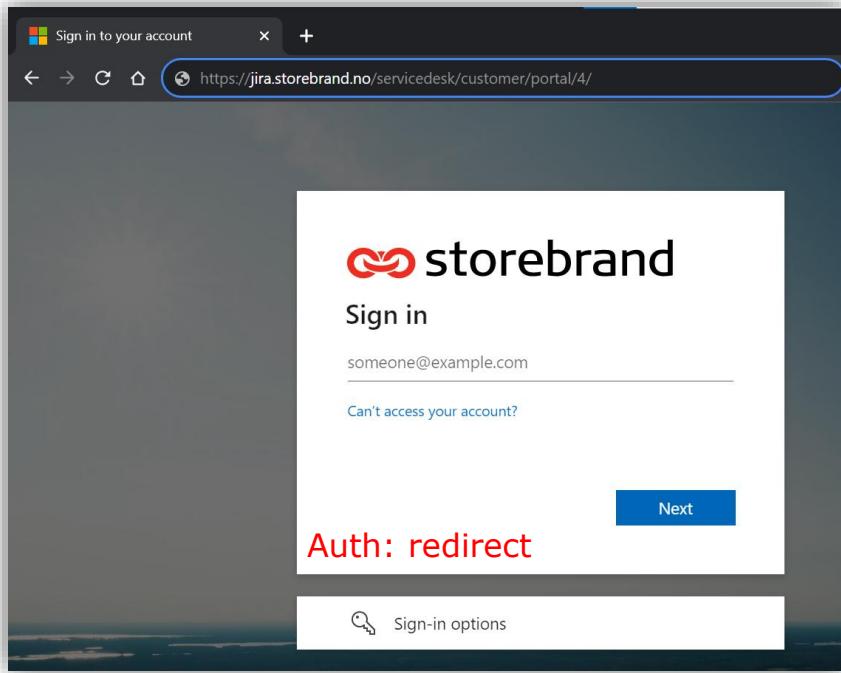
Referrer Policy: strict-origin-when-cross-origin

Response Headers

Cache-Control: no-store, no-cache

Content-Encoding: gzip

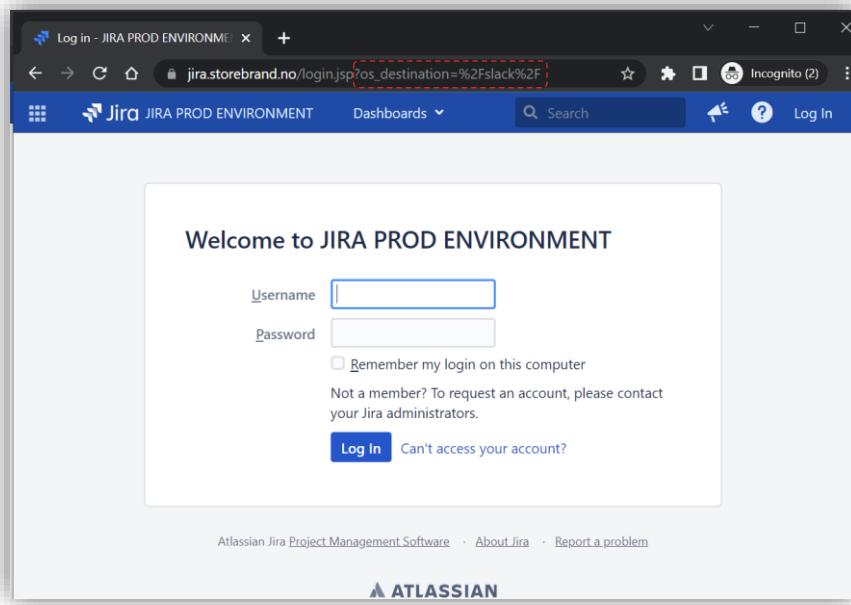
SSO and WAF: expected behavior



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 ENVIRONMENT

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

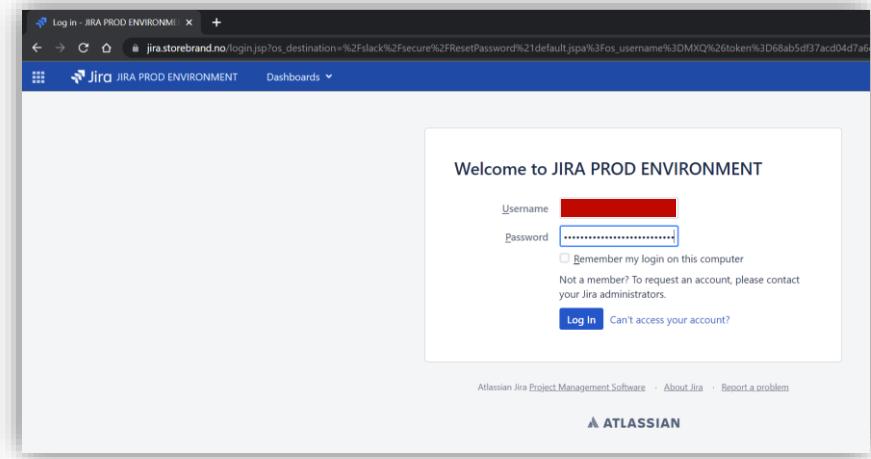
Remember my login on this computer

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 ENVIRONMENT

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

Incognito (2)

Jira JIRA PROD ENVIRONMENT Dashboards

Welcome to JIRA PROD ENVIRONMENT

Username

Password

Remember my login on this computer

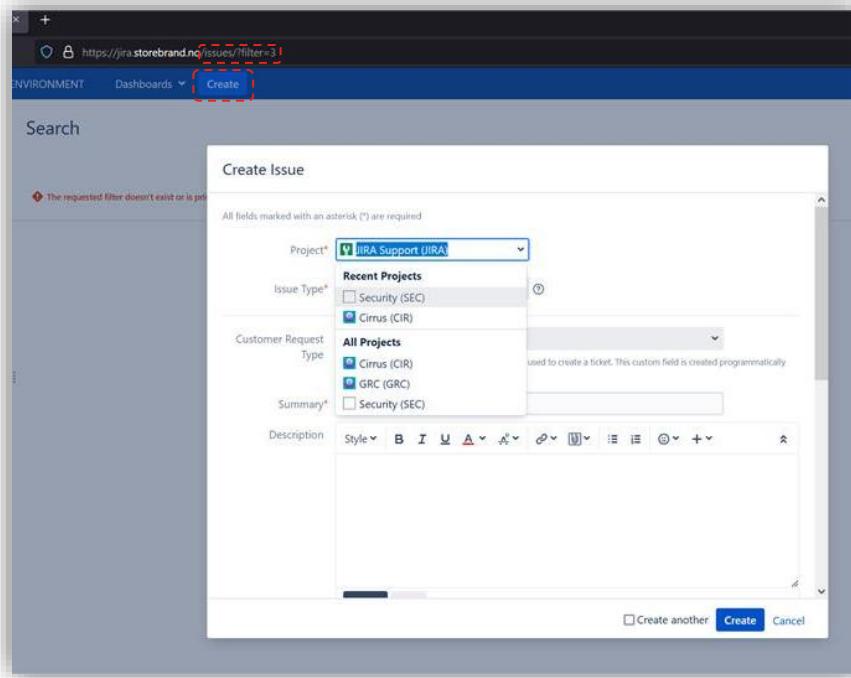
Not a member? To request an account, please contact your Jira administrators.

Log In Can't access your account?

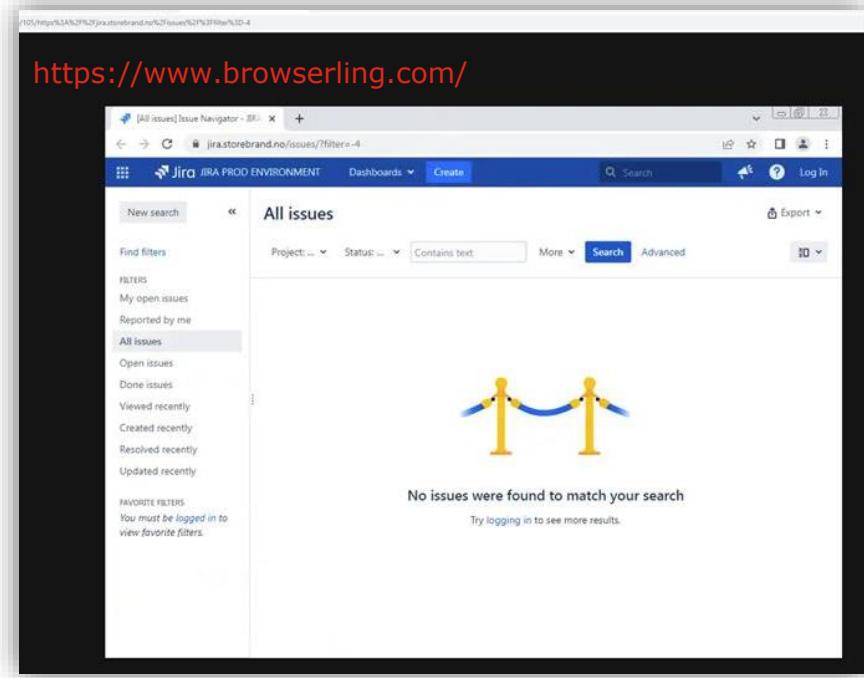
Atlassian Jira Project Management Software · About Jira · Report a problem

ATLASSIAN

Anonymous access: information gathering over the Internet

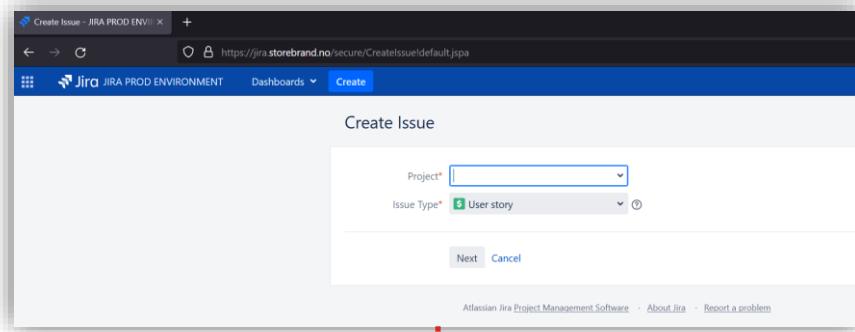


A screenshot of a Jira 'Create Issue' dialog box. The URL in the address bar is <https://jira.storebrand.no/Issues/?filter=3>. The dialog shows fields for 'Project' (set to 'JIRA Support (JIRA)'), 'Issue Type' (Recent Projects: Security (SEC), Cirrus (CIR)), 'Customer Request Type' (All Projects: Cirrus (CIR), GRC (GRC), Security (SEC)), 'Summary' (a text input field), and 'Description' (a rich text editor). A note at the top says 'The requested filter doesn't exist or is not yet defined'. Buttons at the bottom are 'Create another', 'Create', and 'Cancel'.



A screenshot of a Jira 'All issues' search results page. The URL in the address bar is <https://www.browserling.com/>. The page shows a search bar with 'Contains text' and a 'Search' button. A sidebar on the left lists filters: 'All issues' (selected), 'Open issues', 'Done issues', 'Viewed recently', 'Created recently', 'Resolved recently', and 'Updated recently'. A note says 'No issues were found to match your search. Try logging in to see more results.' There is a decorative graphic of two stylized figures holding hands.

Anonymous access: create an issue

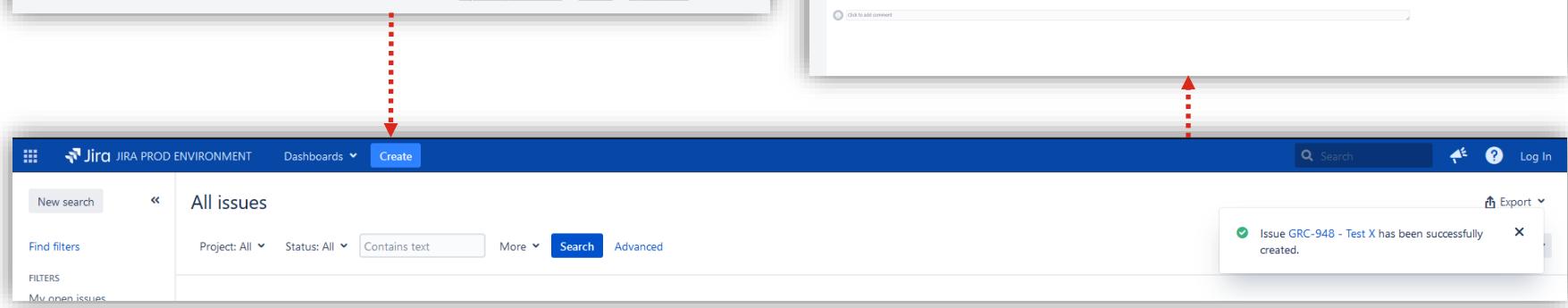


Create Issue

Project:

Issue Type: User story

Next Cancel



New search < All issues

Find filters

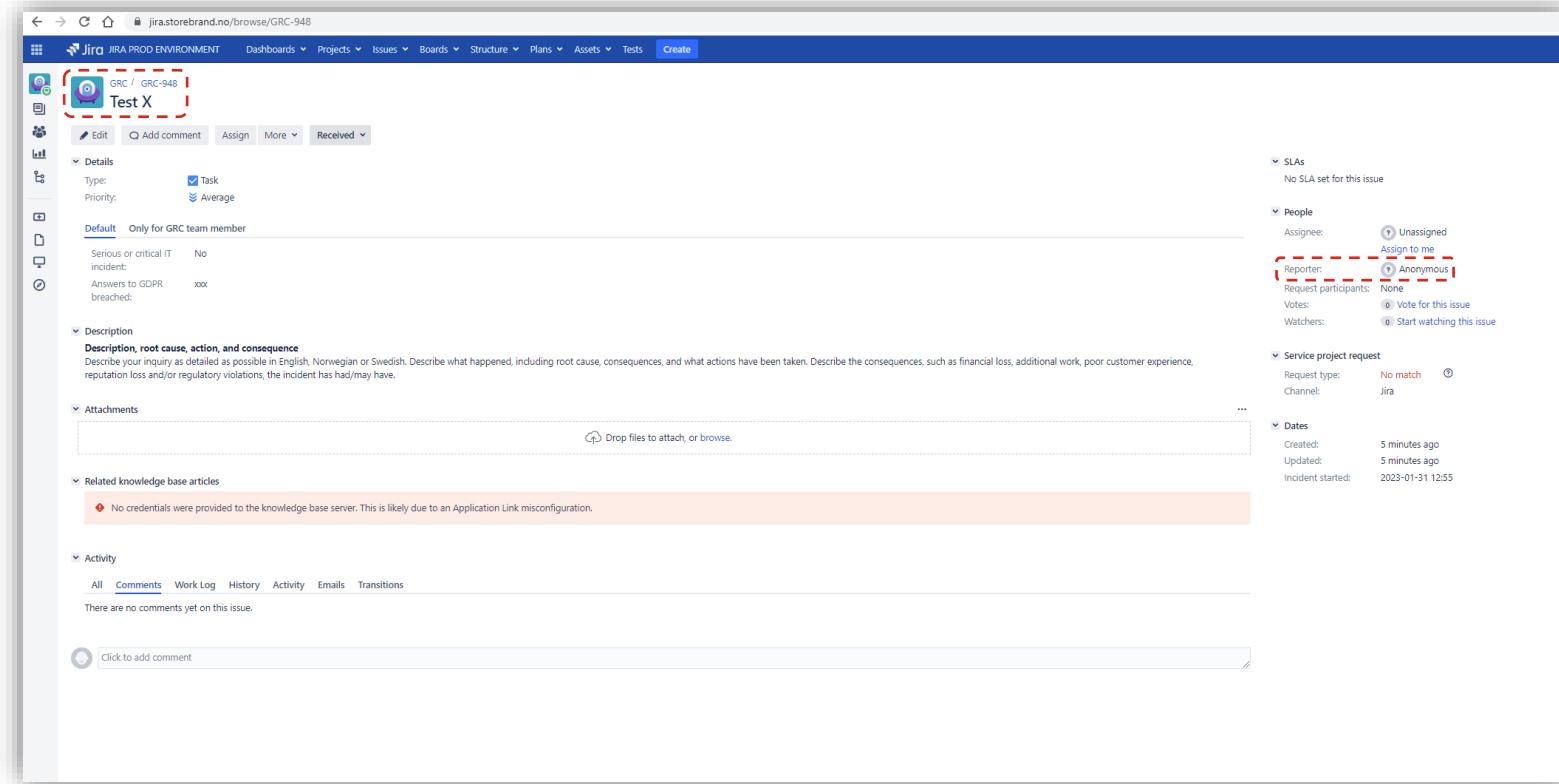
FILTERS

My open issues

Project: All Status: All Contains text More Search Advanced

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

Anonymous access: create an issue



The screenshot shows a Jira issue creation page for an issue titled "Test X". The page is in the "Jira PROD ENVIRONMENT" and the URL is jira.storebrand.no/browse/GRC-948. The issue is a "Task" of "Average" priority, assigned to "Only for GRC team member". The "Details" section shows "Type: Task" and "Priority: Average". The "Description" section contains a detailed description of the incident. The "Attachments" section has a placeholder for file uploads. The "Related knowledge base articles" section shows a red warning message: "No credentials were provided to the knowledge base server. This is likely due to an Application Link misconfiguration." The "Activity" section shows tabs for All, Comments, Work Log, History, Activity, Emails, and Transitions, with the Comments tab selected. The "Comments" section is empty. The "People" section shows the reporter as "Anonymous" and request participants as "None". The "SLAs", "Service project request", and "Dates" sections are also visible.

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

Reputate 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, reputate 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

Comments

Click to add comment

People

Assignee: Unassigned
Reported: Anonymous
Request participants: None
Votes: Vote for this issue
Watchers: Start watching this issue

SLAs

No SLA set for this issue

Service project request

Request type: No match
Channel: Jira

Dates

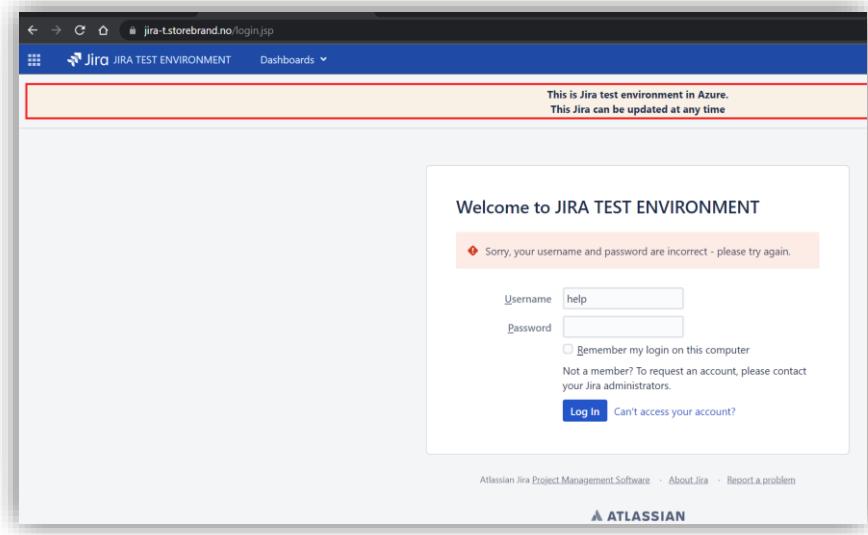
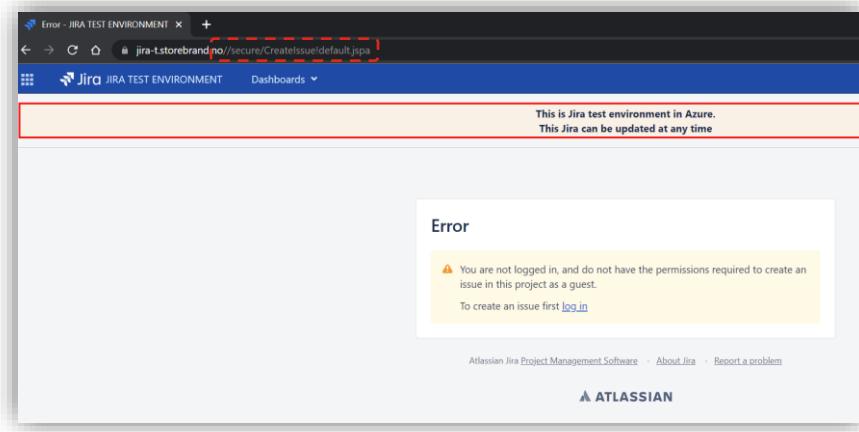
Created: 5 minutes ago
Updated: 5 minutes ago
Incident started: 2023-01-31 12:55

Anonymous access: search for low-hanging fruits

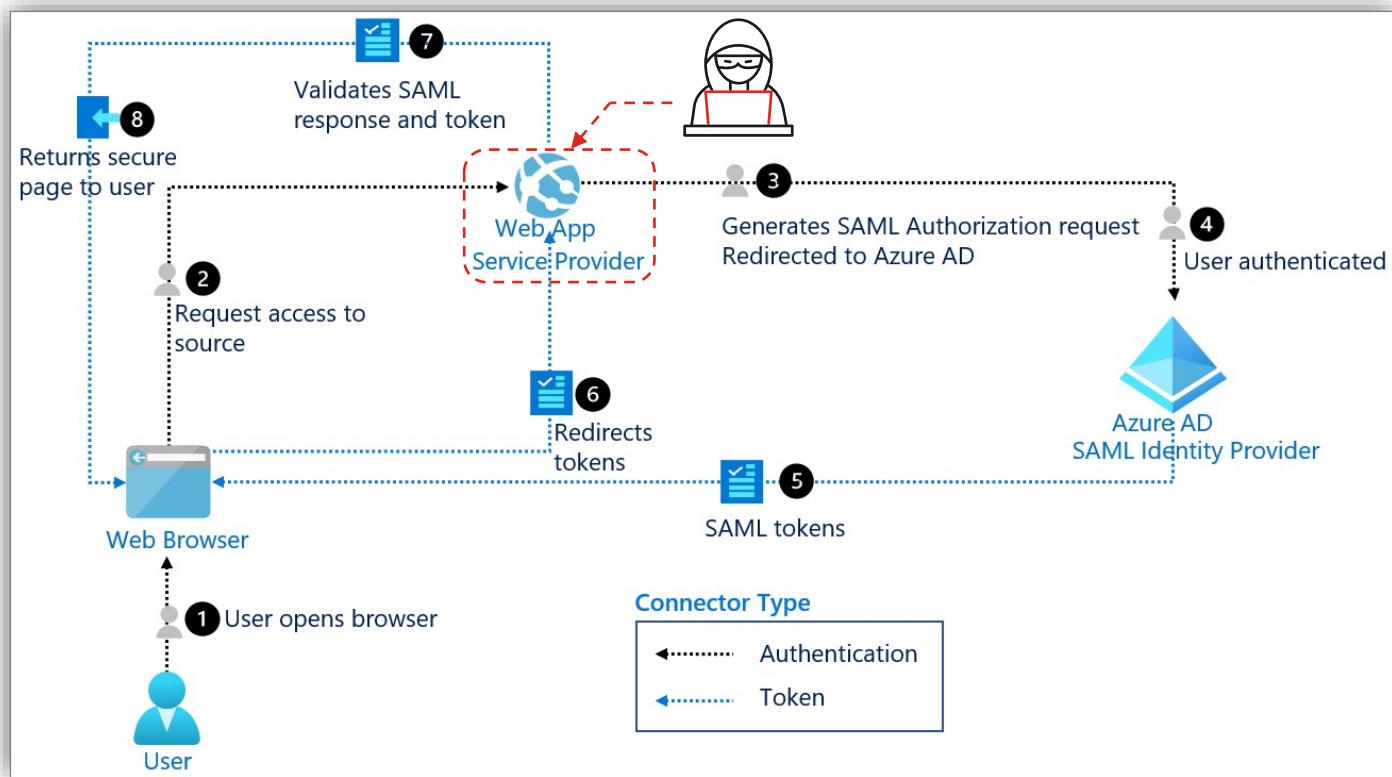
The screenshot shows a Jira search results page with the following details:

- Search Bar:** Contains filters: GRC, Type: All, Status: All, Assignee: All, Contains text: (empty), More, Search, Advanced.
- Issue List:** Shows three issues:
 - GRC-950:** Feil Spot-rate på Auto-FX medfører prisingsavvik på FORNYBAR (20 bp). Status: Received. Details: Type: Task, Priority: None.
 - GRC-948:** Test X. Status: Received.
 - GRC-947:** Feil faktura registrert på feil person. Status: Received.
- Issue Details:** The first issue (GRC-950) is selected. It shows the title, a description, and a summary of its status and details.
- User Menu:** A context menu is open on the right, listing options like Profile, Accessibility, Atlassian Marketplace, MY JIRA HOME, Dashboard, Service project, Boards, Structure, Issue Navigator, Assets, and Log Out.

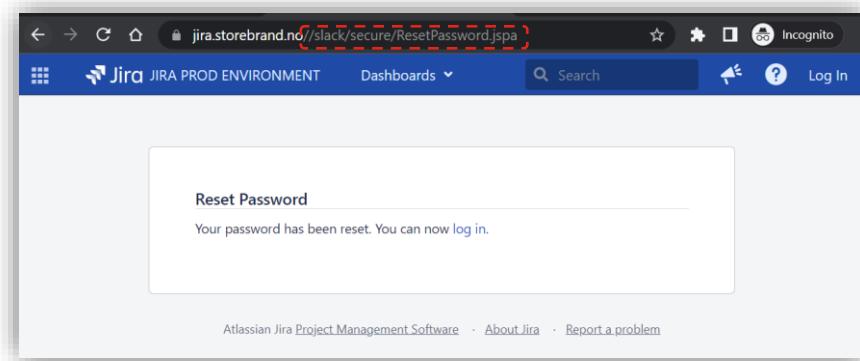
Impact: brute force



SAML authentication with Microsoft Entra ID



Impact: password reset (via Jira)



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=\[REDACTED\]](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=\[REDACTED\]](https://jira.storebrand.no/secure/ForgotLoginDetails.jspa?username=[REDACTED])

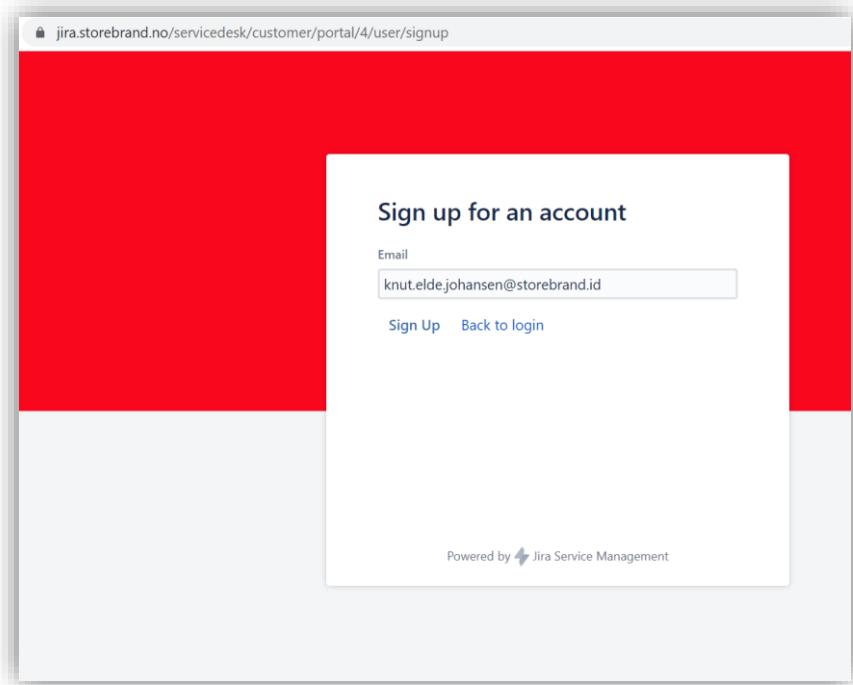
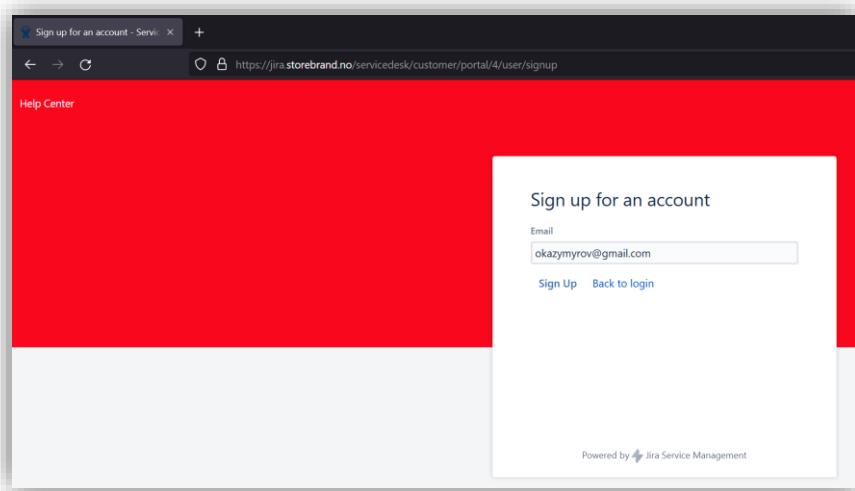
Here are the details of your account:

Username: [REDACTED]

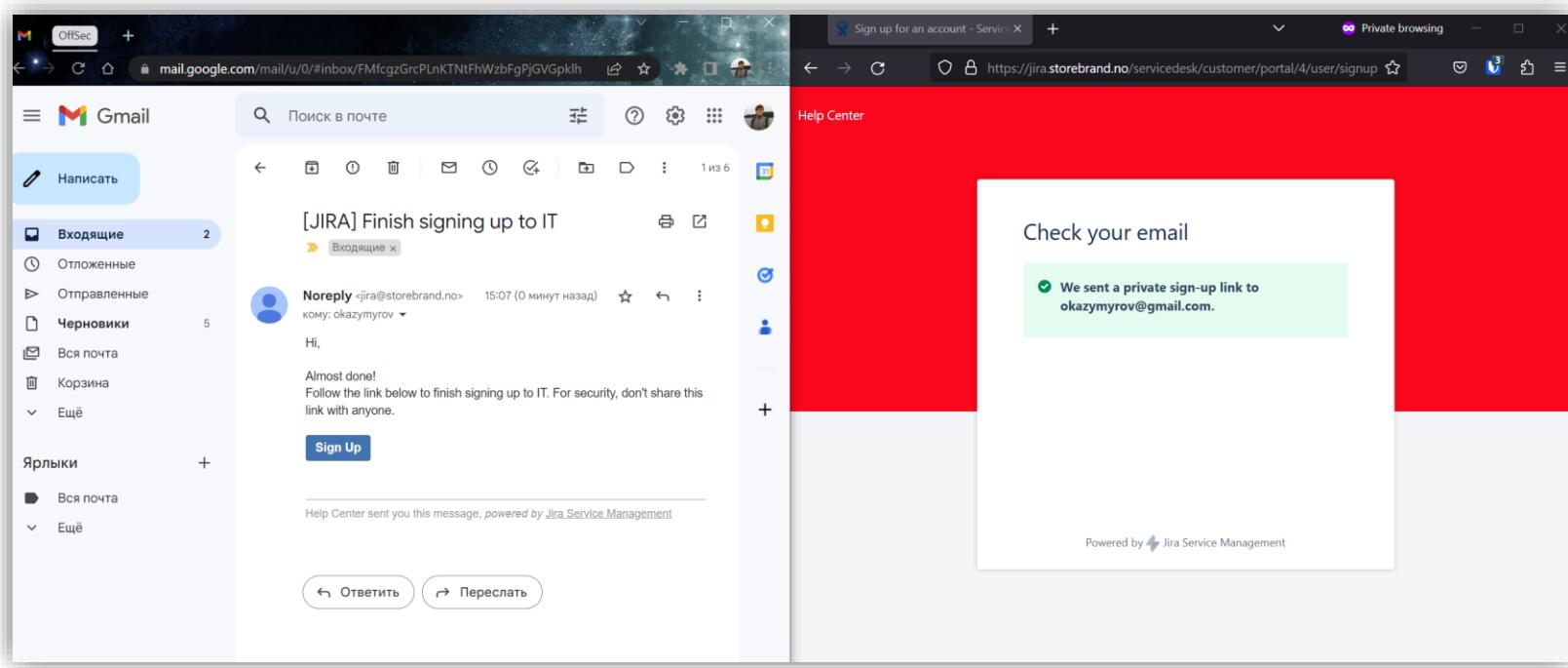
Email: oleksandr.kazymyrov@storebrand.no

Full Name: Kazymyrov, Oleksandr

Impact: sign up for an account



Impact: sign up for an account



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

-  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 a 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/CCoDocs/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.

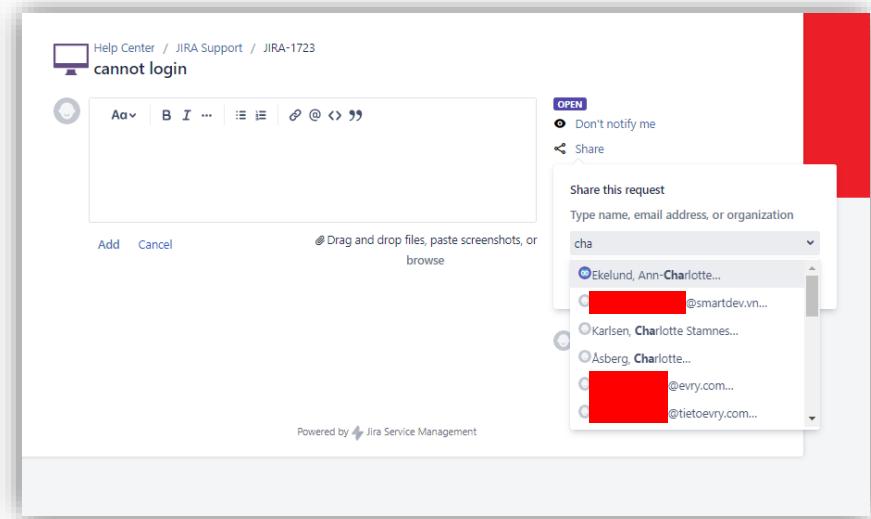
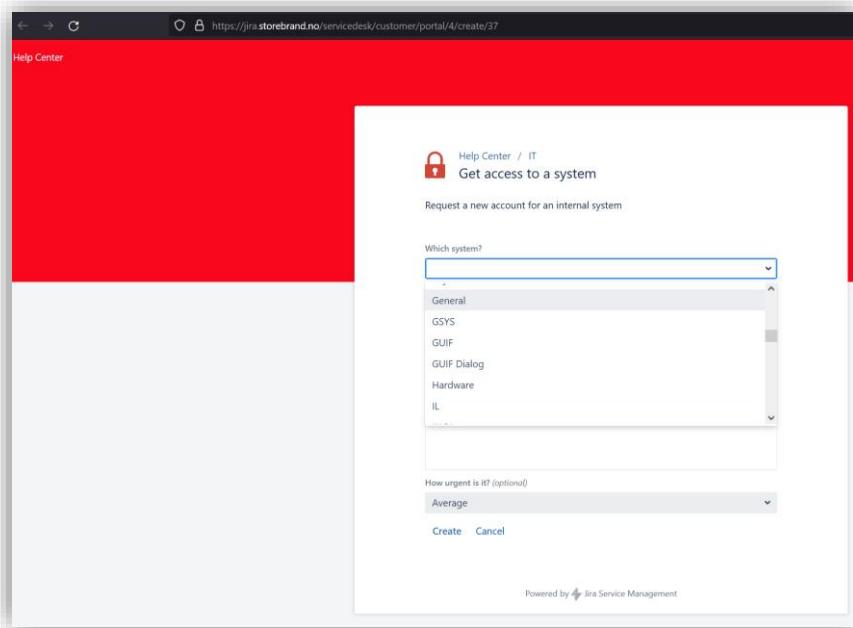
General

CMDB

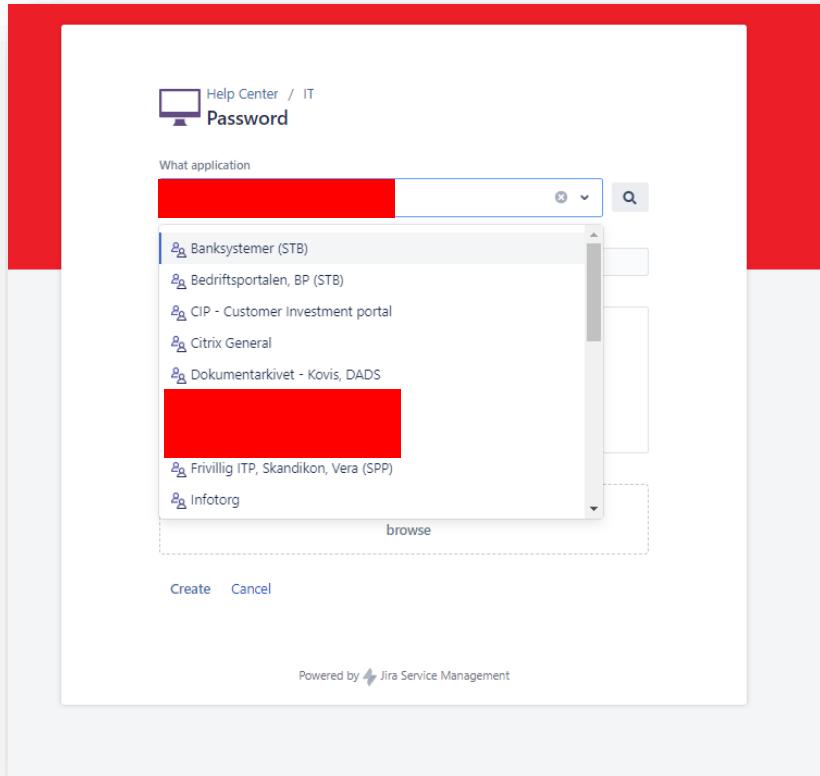
-  Register Azure tagging convention for existing application in CMDB
-  Register a new application in CMDB

Powered by  Jira Service Management

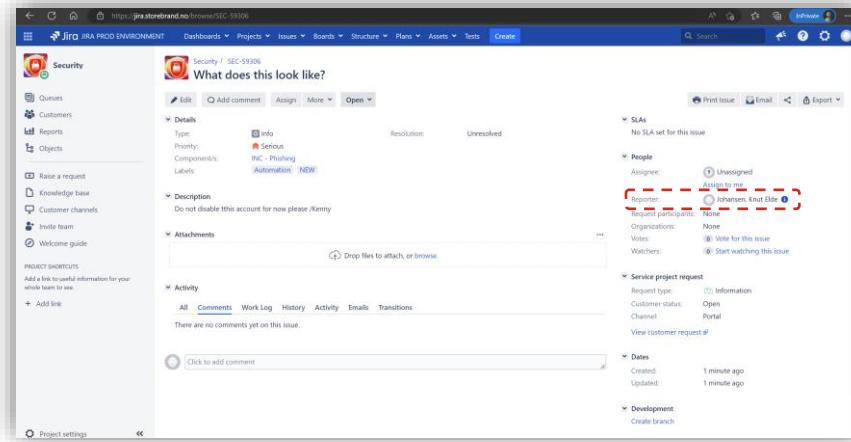
Impact: enumeration / reconnaissance



Impact: social engineering via IT support



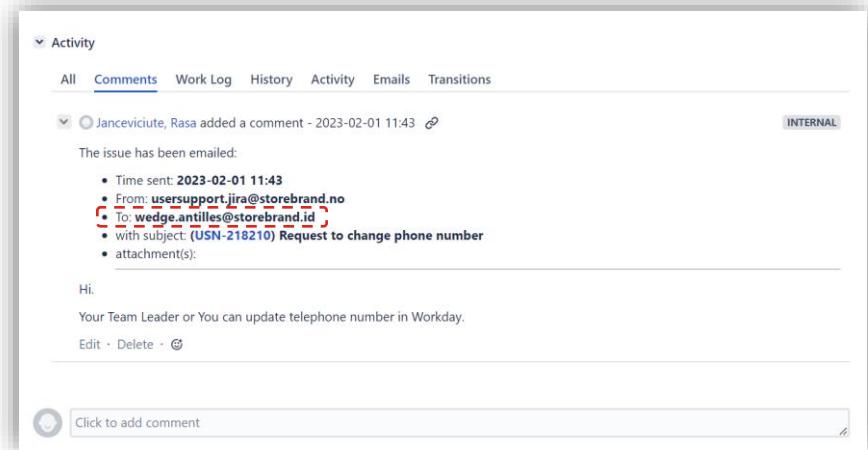
Impact: social engineering via IT support



The screenshot shows a Jira issue page for a service request. The issue is titled "What does this look like?". The details section shows the following information:

- Type: Service
- Priority: High
- Components: the - Printing
- Labels: Automation - NEW
- Description: Do not disable this account for now please /Kenny
- Attachments: None
- SLA: No SLA set for this issue
- People: Assignee: Unassigned, Request participant: None, Organization: None, Votes: None, Watchers: None
- Service project request: Request type: Information, Customer status: Open, Channel: Portal, View customer request: None
- Dates: Created: 1 minute ago, Updated: 1 minute ago
- Development: Create branch

The page also includes a sidebar with project shortcuts and a "Click to add comment" button.



The screenshot shows the Jira activity feed. A comment from "Janceviciute, Rasa" was added on 2023-02-01 11:43. The comment text is:

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):

The comment is marked as "INTERNAL". Below the comment, there is a message from "Hi." and a note: "Your Team Leader or You can update telephone number in Workday." with a "Edit" link.

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

Shared with
 Torsbakken, Stig Tombre
Creator

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

Impact: social engineering via IT support

Help Center / JIRA Support / JIRA-1723

cannot login


<script>alert(1)</script>

OPEN Don't notify me
 Share

Shared with

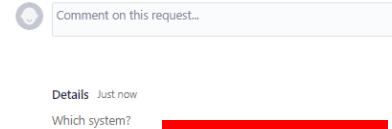
-  **FakeUser** Creator
-  **Bergerud, Øyvind** Remove
-  **Torsbakken, Stig Tombre** Remove

3109c18d-f607-49c...

Add Cancel 

Powered by Jira Service Management

Help Center / IT / USN-218162


I need read access please for user Fl2

ANALYZE Don't notify me
 Share

Details Just now

Which system?
Admincontrol, Citrix [REDACTED]

Why do you need this?
I need read access please for user Fl2

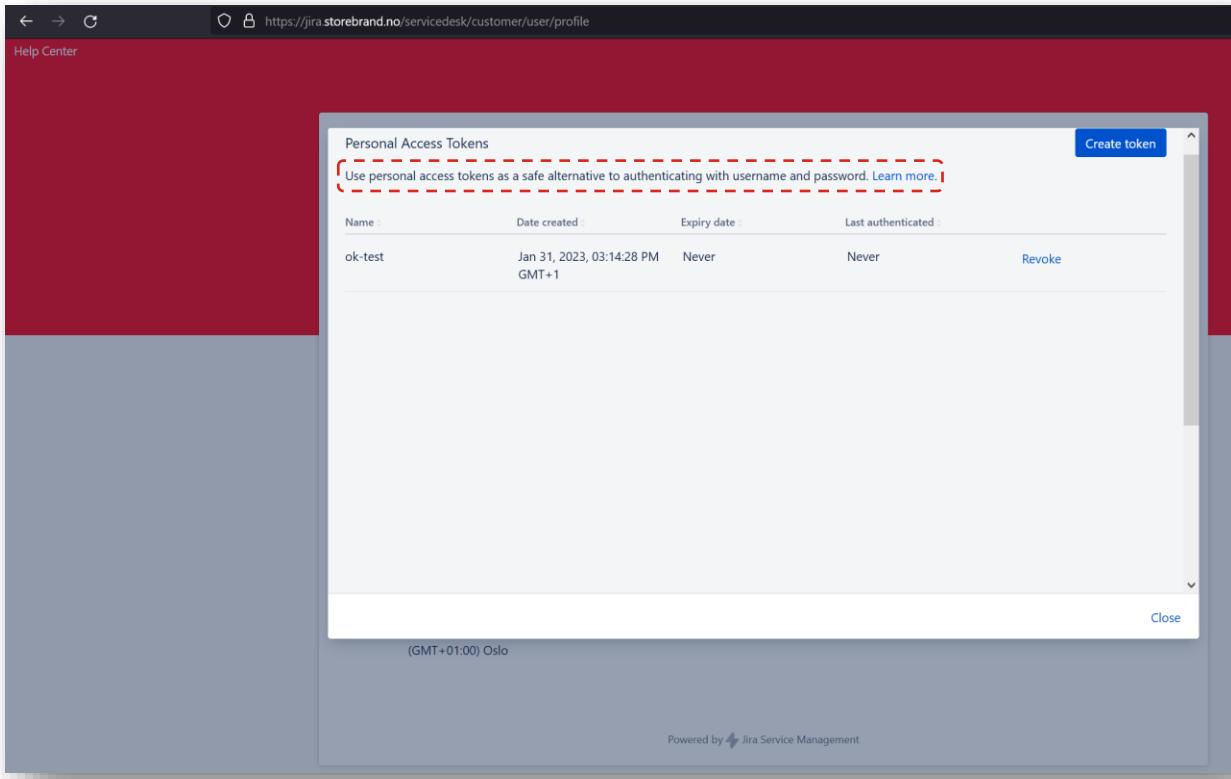
How urgent is it?
Average

Shared with

-  **S** Creator

Powered by Jira Service Management

Impact: backdoor

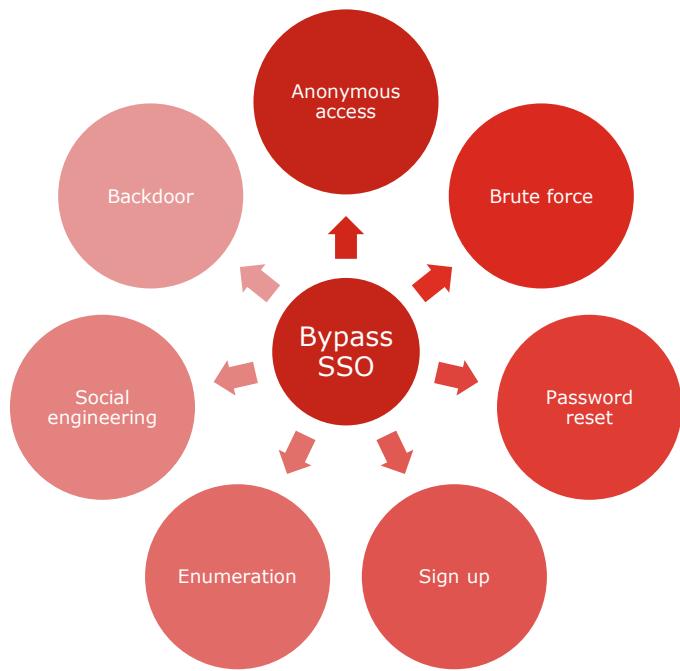


A screenshot of a web browser displaying a Jira Service Management interface. The URL in the address bar is <https://jira.storebrand.no/servicedesk/customer/user/profile>. The page title is "Help Center". A modal window is open, titled "Personal Access Tokens". The modal contains a sub-headline: "Use personal access tokens as a safe alternative to authenticating with username and password. [Learn more.](#)". A table lists a single token entry:

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

At the bottom of the modal, there is a "Close" button and a note: "(GMT+01:00) Oslo".

Summary of impact





”

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

Confucius