

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

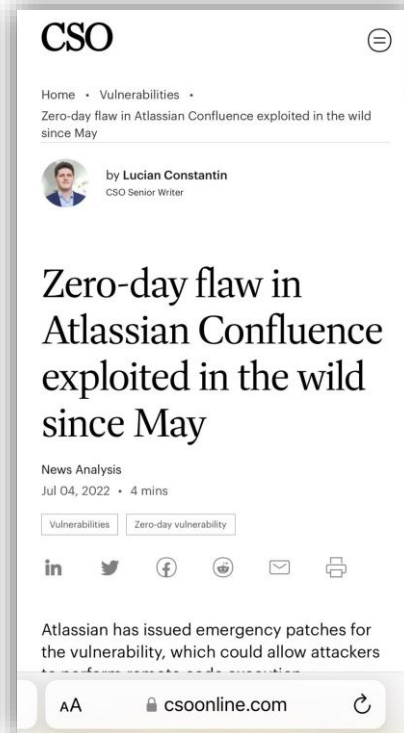
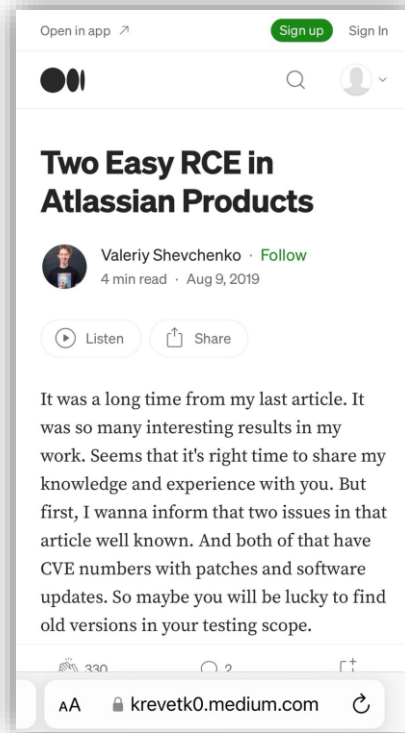
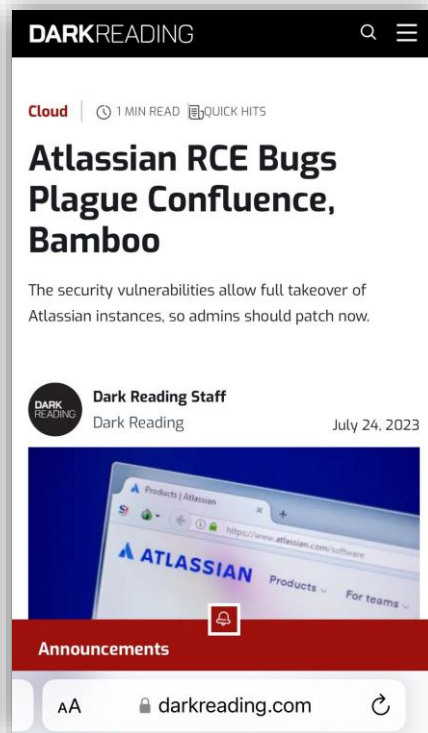
Bli med for å se profilen



Who am I?



Atlassian in security news



[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.

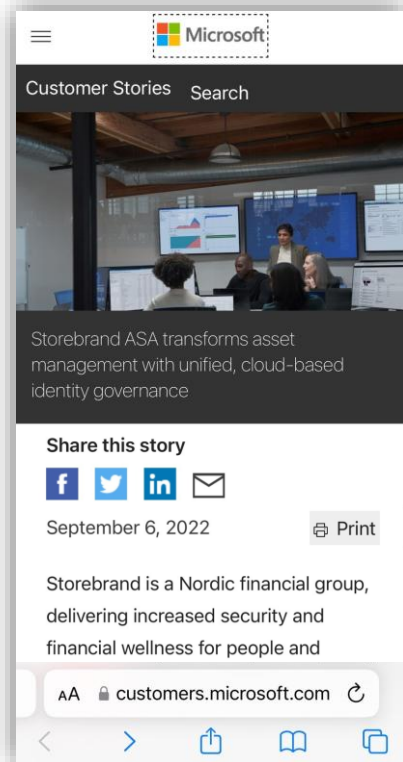
Atlassian in security news

Versions prior to 8.0.0 are not affected by this vulnerability.

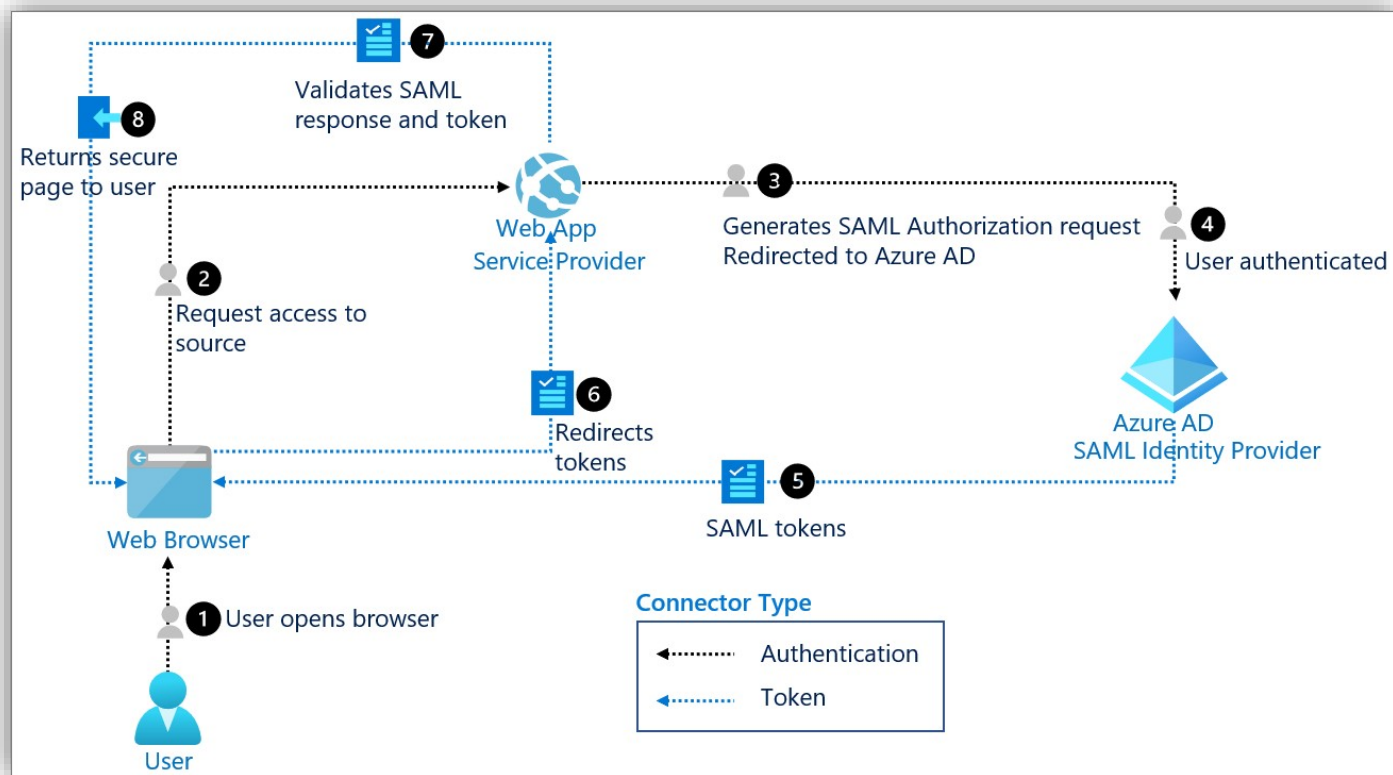
Product	Affected Versions
Confluence Data Center and Confluence Server	<ul style="list-style-type: none">• 8.0.0• 8.0.1• 8.0.2• 8.0.3• 8.0.4• 8.1.0• 8.1.1• 8.1.3• 8.1.4• 8.2.0• 8.2.1• 8.2.2• 8.2.3• 8.3.0• 8.3.1• 8.3.2• 8.4.0• 8.4.1• 8.4.2• 8.5.0• 8.5.1

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

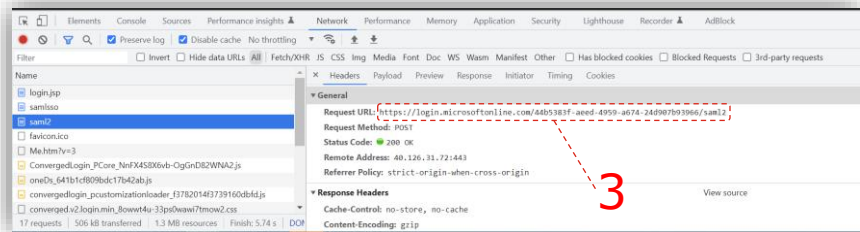
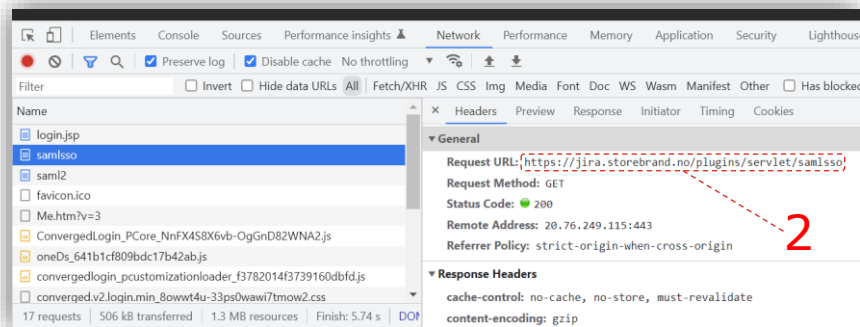
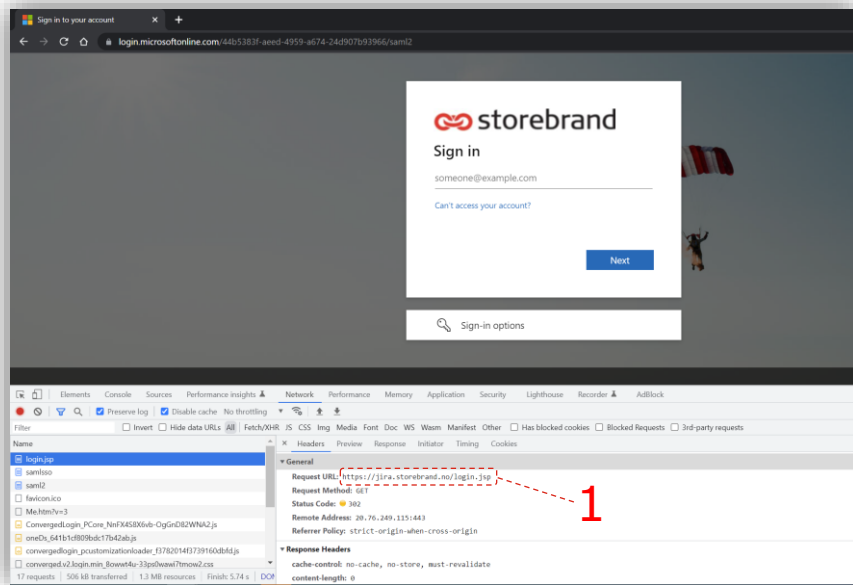
Storebrand in the cloud



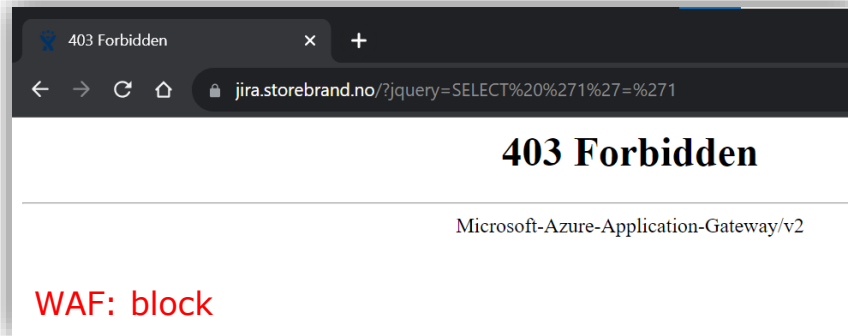
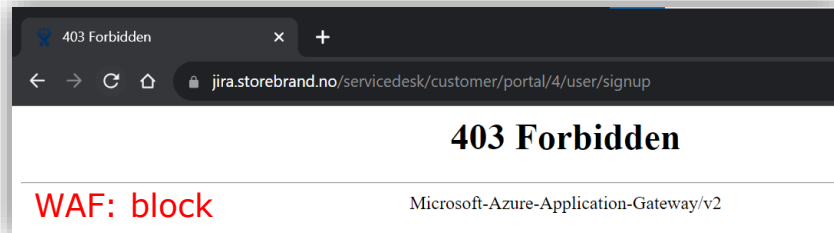
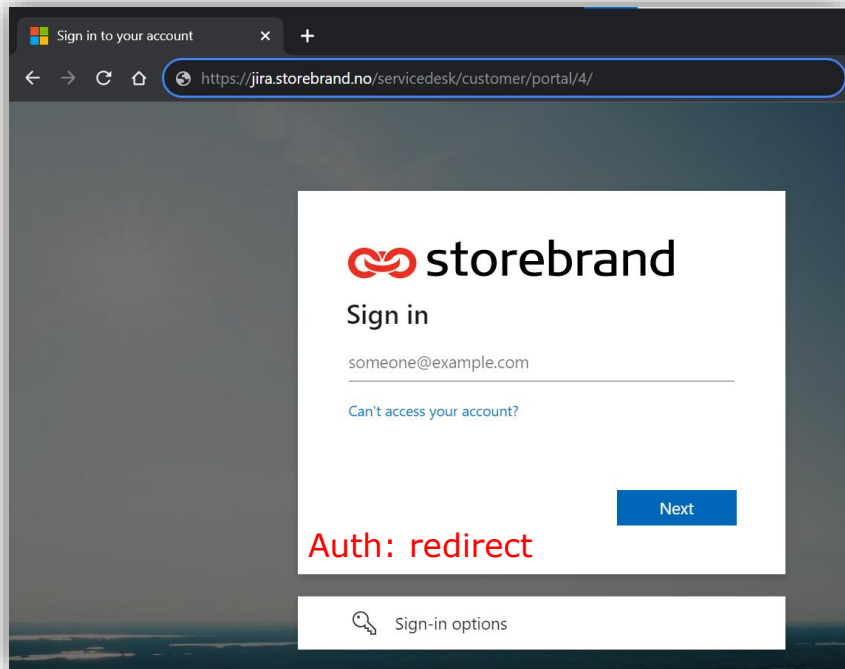
SAML authentication with Microsoft Entra ID



Azure AD: first steps in the authentication flow



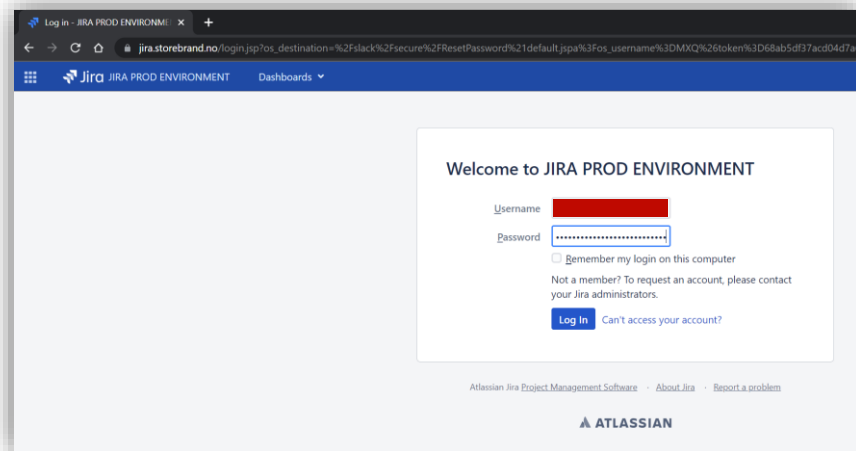
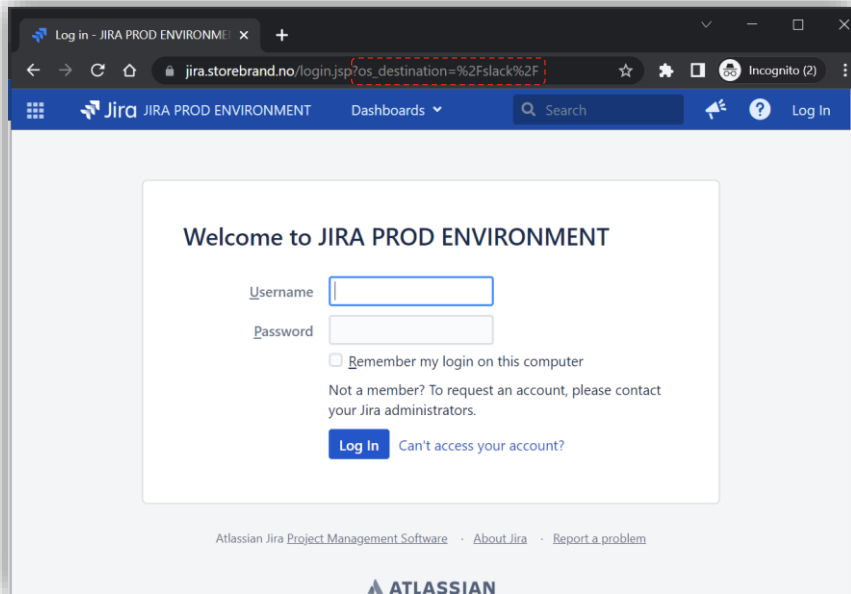
SSO and WAF: expected behavior



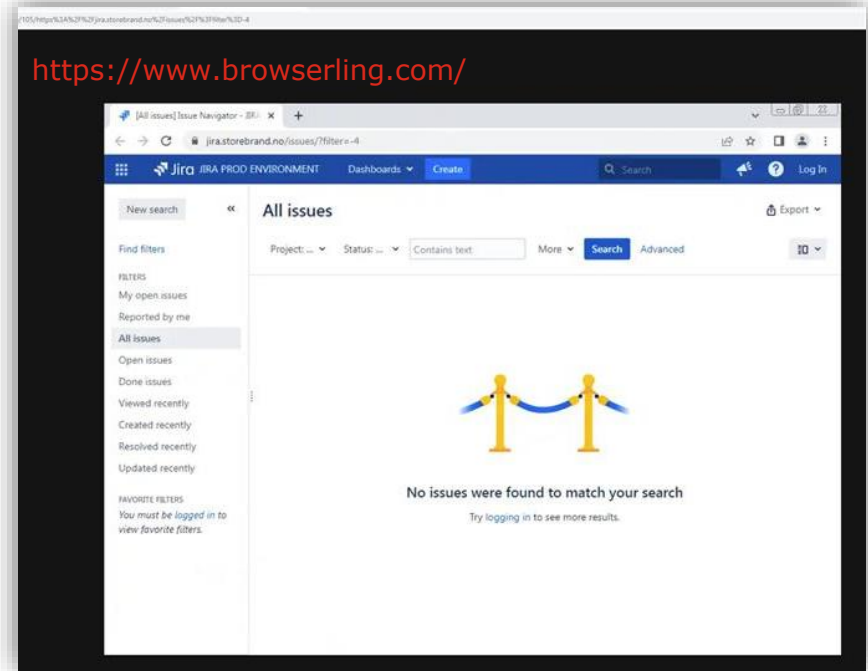
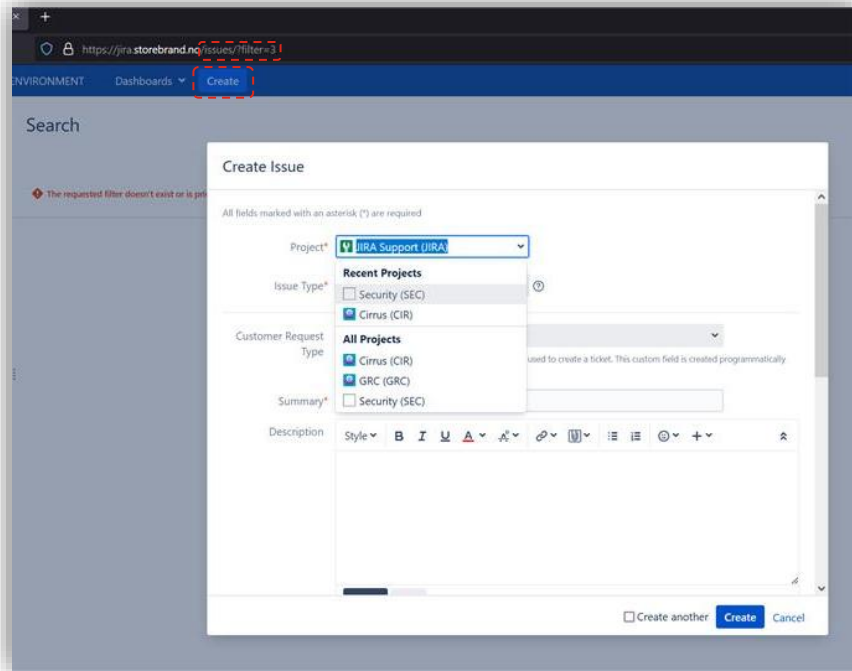
Bypass SSO

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



Anonymous access: information gathering over the Internet



Anonymous access: create an issue

Create Issue - JIRA PROD ENVIRONMENT

https://jira.storebrand.no/secure/Createlssue/default.jspa

JIRA PROD ENVIRONMENT Dashboards Create

Create Issue

Project*

Issue Type*

Next Cancel

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

JIRA PROD ENVIRONMENT

Text X - GRC-948

To Do

add comment Assign More ...

Details

Type: Text

Priority: Average

Description

Only for GRC team member

Service or critical IT incident

Answers to GRC incidents

Attachments

Drop files to attach, or browse

Related knowledge base article

No incidents 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

Labels

None

People

Assignee: Unassigned

Reporter: Anonymous

Watchers

Start watching this issue

Service project request

Request type: No match

Channel: N/A

Details

Created: 3 minutes ago

Updated: 3 minutes ago

Incident created: 2023-01-11 12:05

JIRA PROD ENVIRONMENT Dashboards Create

New search

Find filters

FILTERS

My open issues

All issues

Project: All Status: All Contains text More Search Advanced

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

Anonymous access: create an issue

The screenshot shows the Jira issue page for 'Test X' in the 'GRC / GRC-948' project. The page is titled 'Test X' and has a status of 'Task'. The 'Reporter' field is highlighted with a red dashed box, showing 'Anonymous'. The 'Assignee' field is also highlighted with a red dashed box, showing 'Unassigned'. The 'Request participants' field shows 'None'. The 'Votes' field shows '0' and the 'Watchers' field shows '0'. The 'Service project request' section shows 'Request type: No match' and 'Channel: Jira'. The 'Dates' section shows 'Created: 5 minutes ago', 'Updated: 5 minutes ago', and 'Incident started: 2023-01-31 12:55'. The 'Description' section contains the text: '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.' The 'Attachments' section shows a message: 'No credentials were provided to the knowledge base server. This is likely due to an Application Link misconfiguration.' The 'Activity' section shows 'All Comments Work Log History Activity Emails Transitions' and 'There are no comments yet on this issue.'

Anonymous access: search for low-hanging fruits

The screenshot displays the Jira PROD ENVIRONMENT interface. The top navigation bar includes links for Dashboards, Projects, Issues, Boards, Structure, Plans, Assets, Tests, and a Create button. A search bar is located on the right. The main content area shows a search results page for the issue 'Feil Spot-rate på Auto-FX medfører prisingsavvik på FORNYBAR (20 bp)'. The issue details include a Type of Task, Priority of None, and SLAs of 2d 7h and 1mo. A sidebar on the left lists filters such as 'My open issues', 'Reported by me', 'All issues', 'Open issues', 'Done issues', 'Viewed recently', 'Created recently', and 'Resolved recently'. A dropdown menu is open on the right, showing options like Profile, Accessibility, Atlassian Marketplace, MY JIRA HOME, Dashboard, Service project, Boards, Structure, Issue Navigator, Assets, and Log Out.

Jira PROD ENVIRONMENT

Search

GRC / GRC-950

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

Type: Task

Priority: None

SLAs

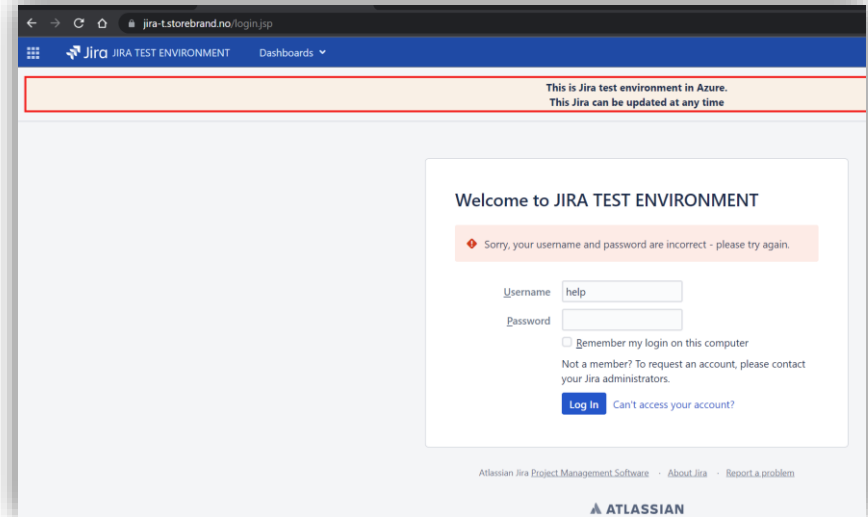
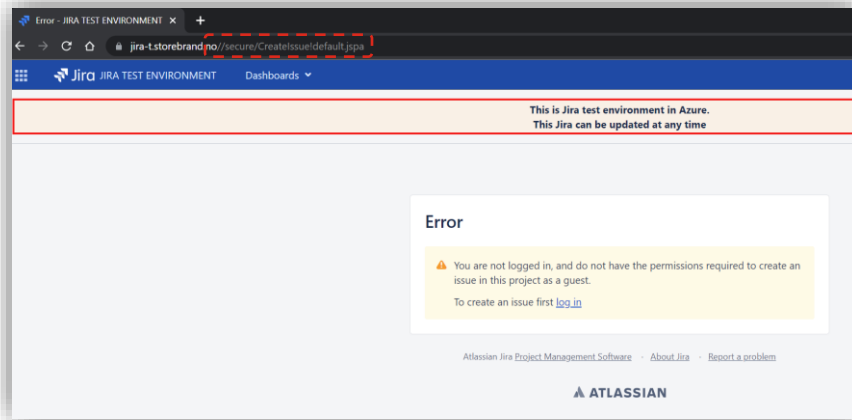
2d 7h

1mo

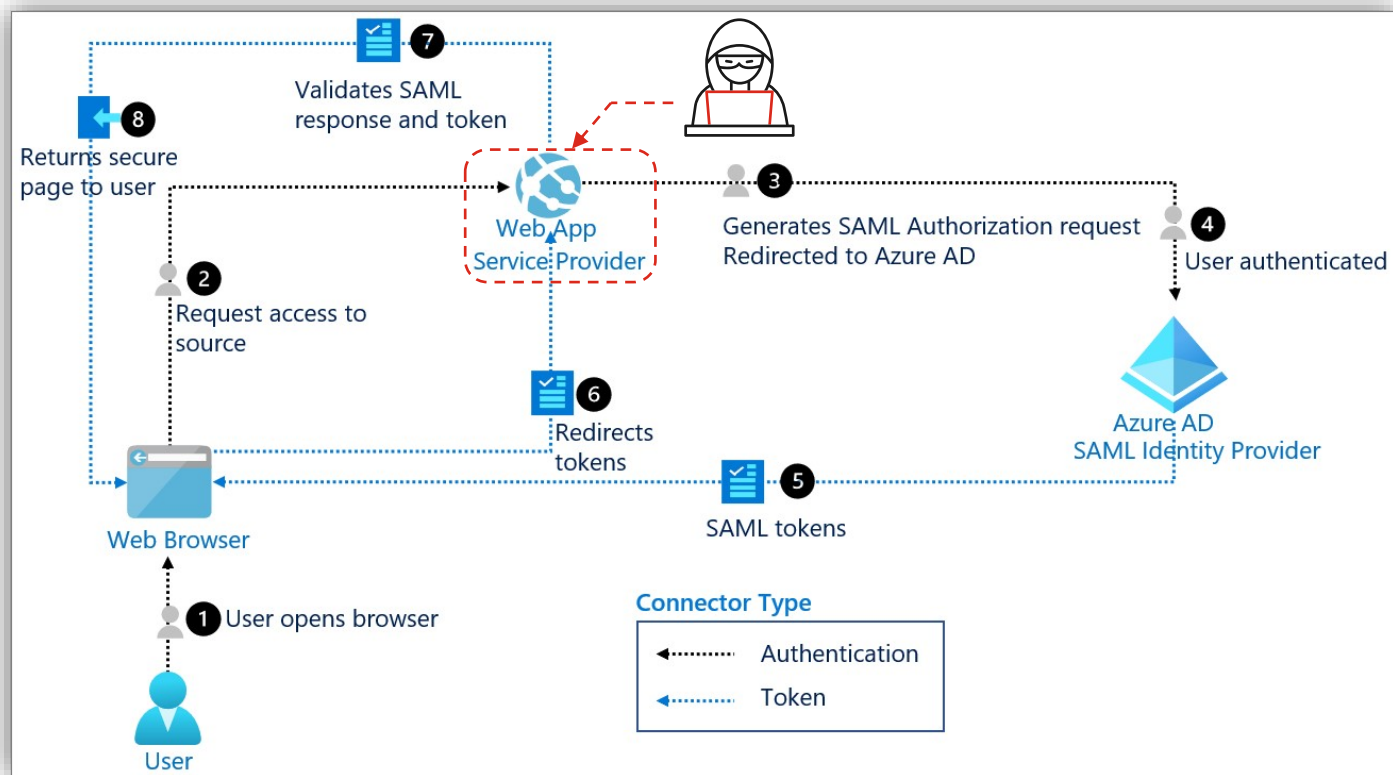
Time to start within 2d 8h

Time to done within 1 month

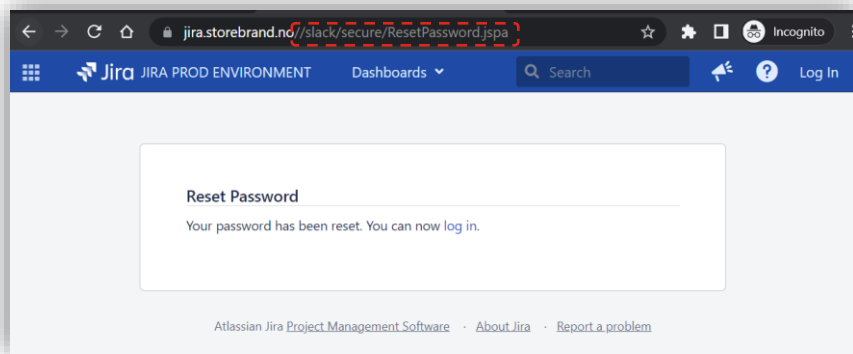
Impact: brute force



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?](https://jira.storebrand.no/secure/ResetPassword!default.jspa?os_username=[REDACTED])

[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])

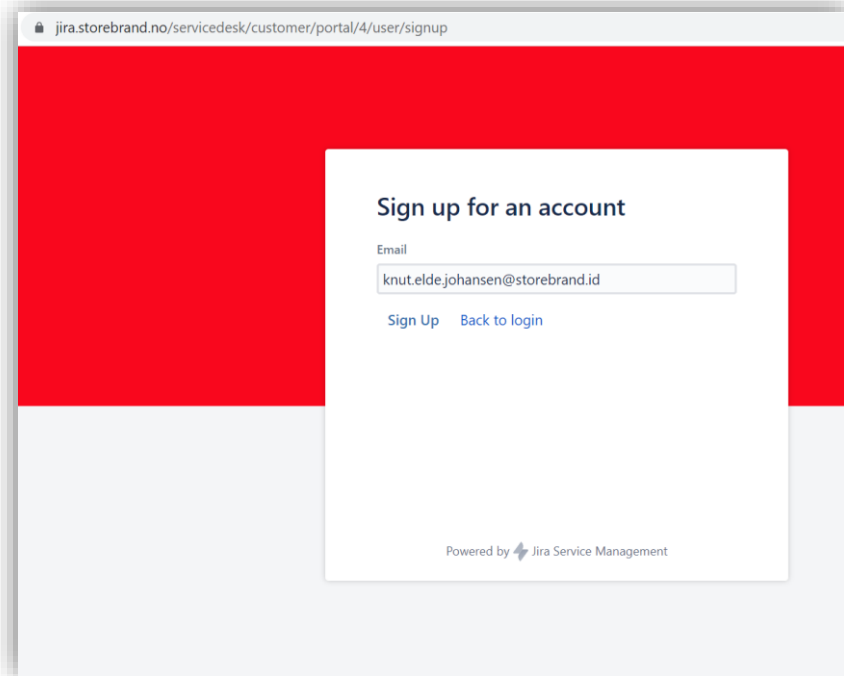
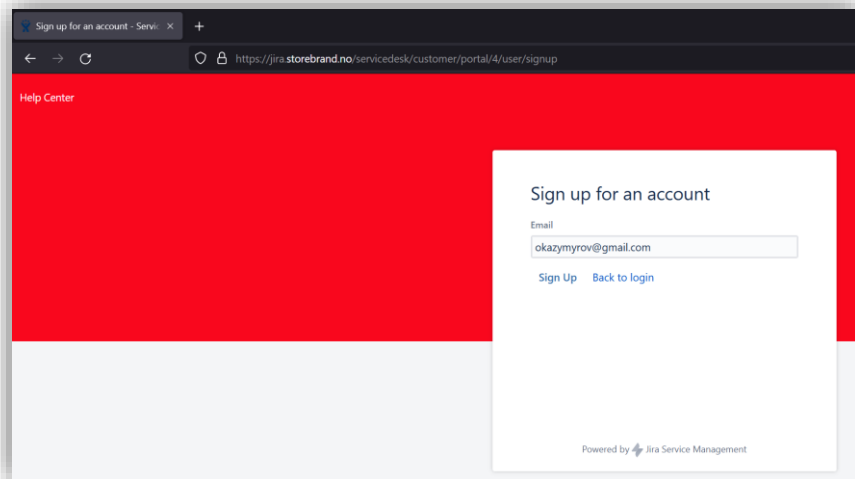
Here are the details of your account:

Username: [REDACTED]

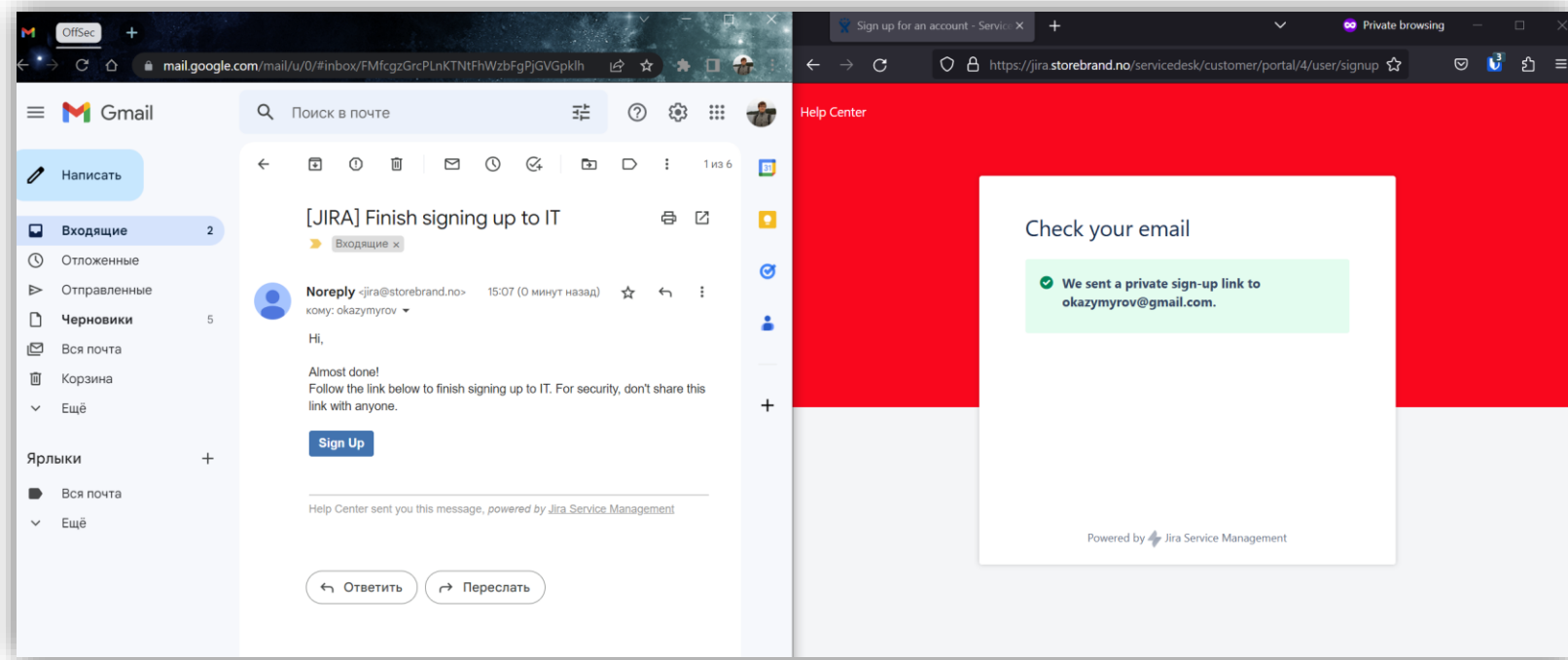
Email: oleksandr.kazymyrov@storebrand.no

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


CMD8


 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

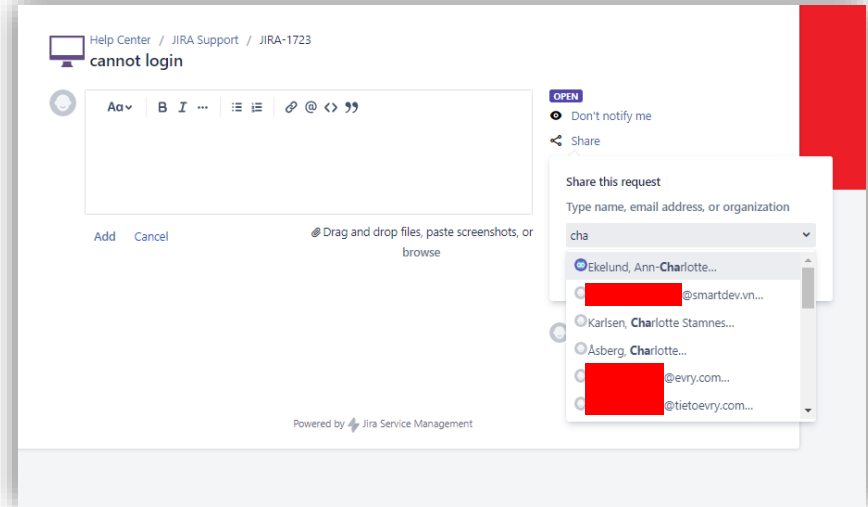
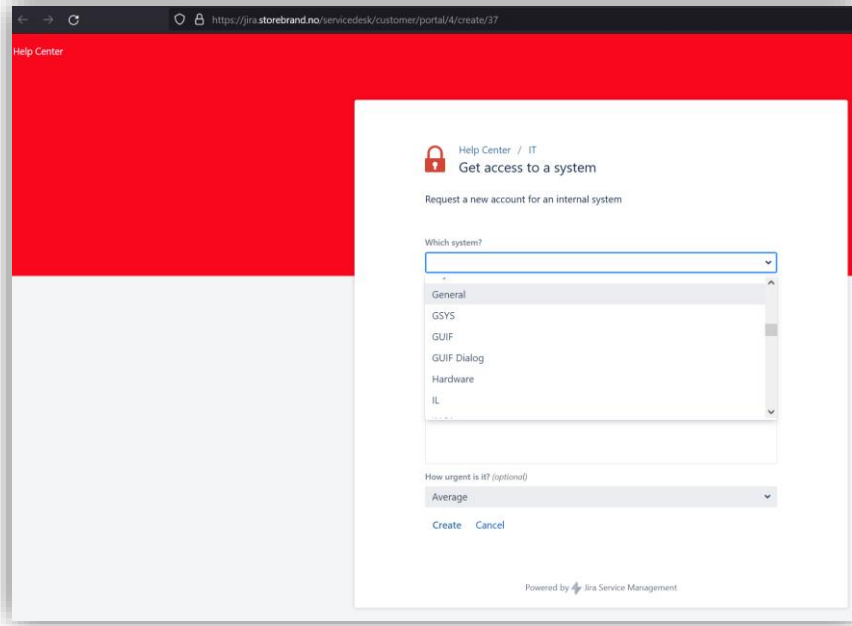
CMD8

 Register Azure tagging convention for existing application in CMD8

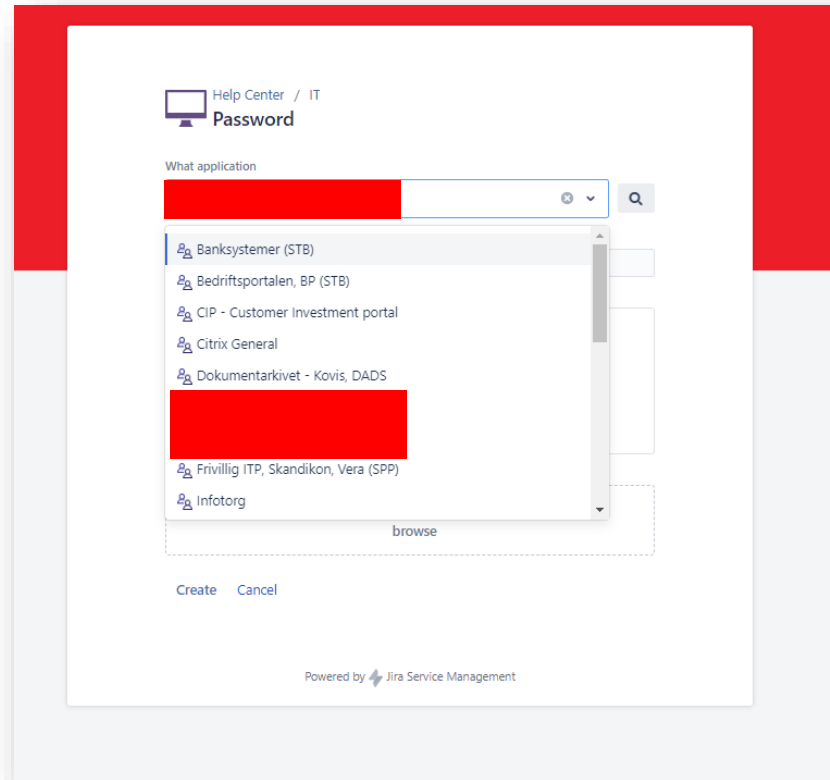
 Register a new application in CMD8

Powered by  Jira Service Management

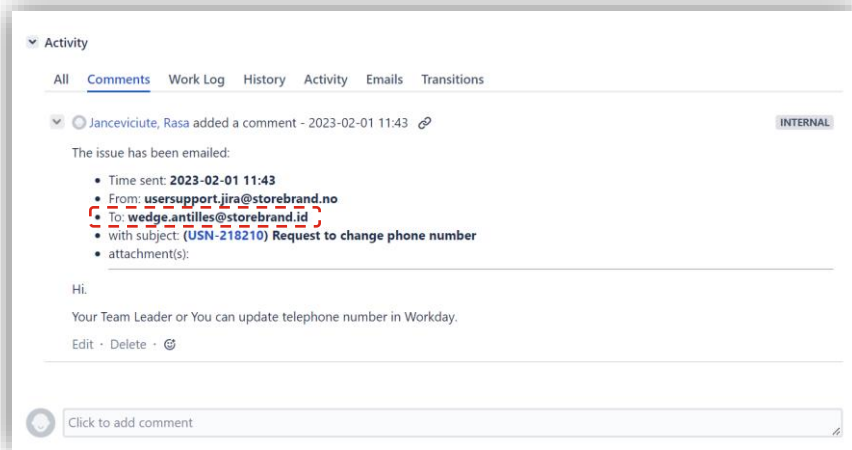
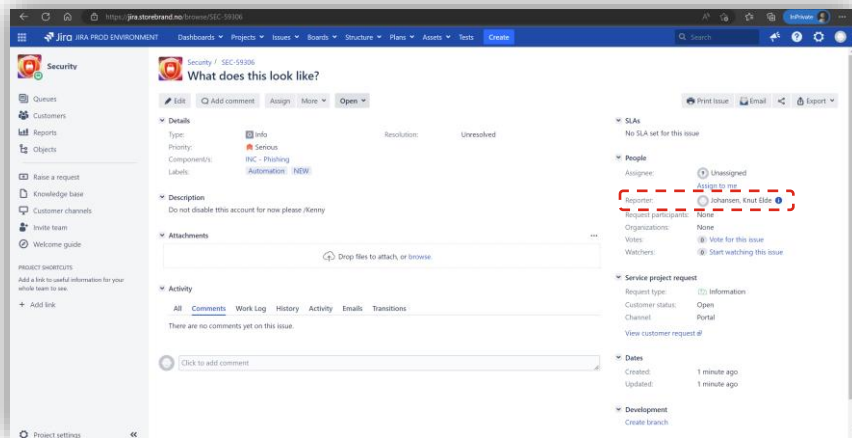
Impact: enumeration / reconnaissance




Impact: social engineering via IT support




Impact: social engineering via IT support




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

OPEN

- Don't notify me
- Share

Shared with

- FakeUser
Creator
- Bergerud, Øyvind
[Remove](#)
- Torsbakken, Stig Tombre
[Remove](#)

3109c18d-f607-49c...

[Add](#) [Cancel](#)

Drag and drop files, paste screenshots, or [browse](#)

Powered by Jira Service Management

Help Center / IT / USN-218162

I need read access please for user FI2

ANALYZE

Comment on this request...

- Don't notify me
- Share

Shared with

- S
Creator

Details Just now

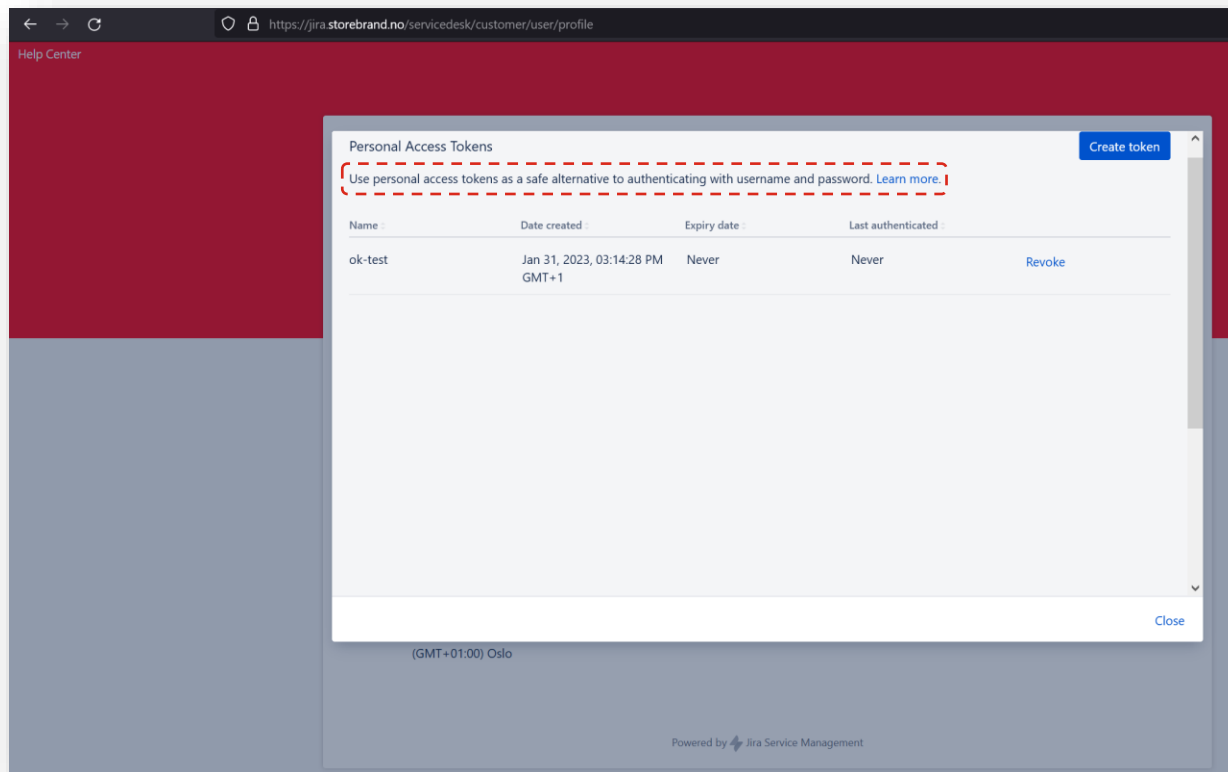
Which system?
Admincontrol, Citrix, [REDACTED]

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

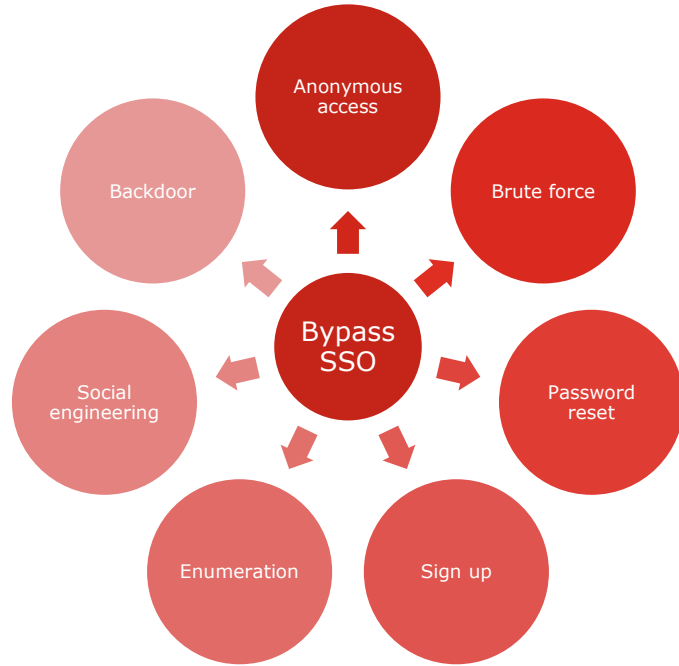
How urgent is it?
Average

Powered by Jira Service Management

Impact: backdoor



Summary of impact





”

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

Confucius