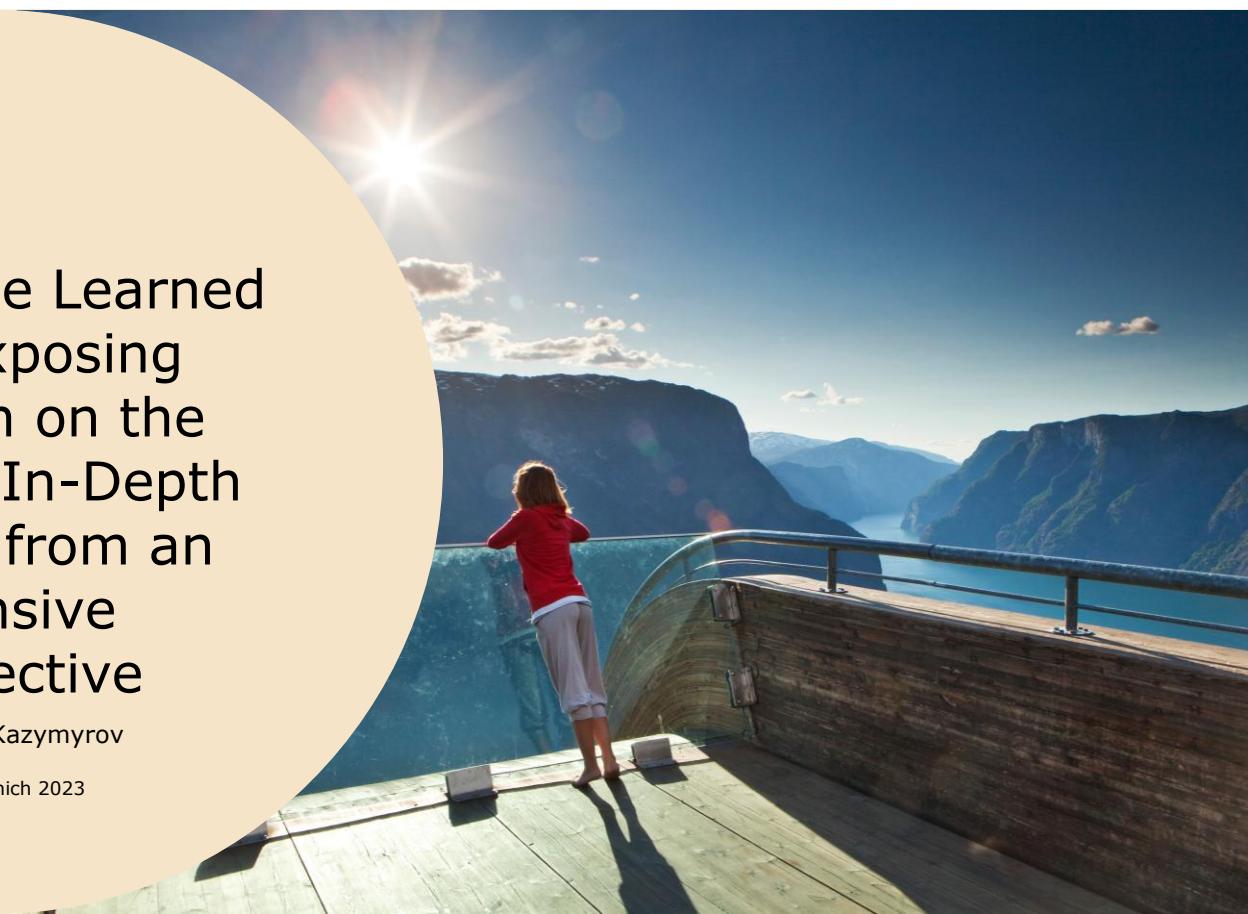


What We've Learned from Exposing Atlassian on the Internet: In-Depth Analysis from an Offensive Perspective

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.

 [thehackernews.com](https://thehackernews.com/2021/09/atlassian-confluence-rce-flaw-abused.html) 

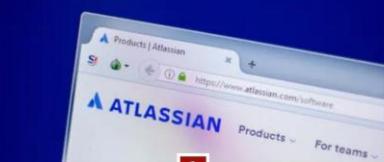
DARKREADING  

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

 [darkreading.com](https://darkreading.com/atlassian-rce-bugs-plague-confluence-bamboo/) 

[Open in app](#)  

Two Easy RCE in Atlassian Products

 Valeriy Shevchenko · [Follow](#)
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.

 [krevetk0.medium.com](https://krevetk0.medium.com/two-easy-rce-in-atlassian-products-330) 

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

[Vulnerabilities](#) [Zero-day vulnerability](#)



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

 [csonline.com](https://csonline.com/zero-day-flaw-in-atlassian-confluence-exploited-in-the-wild-since-may/) 

[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

Microsoft

Pulse ▾

TRANSFORMER
BEDRIFTSOPTIMALISERING

Storebrand flyttet over 1000 milliarder kroner til skyen med Azure

f t in e m

AA 🔒 pulse.microsoft.com

< > ↗ ↘ ↗ ↘

E24 | Børs Bilabonnement

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

f t in e

September 6, 2022

Print

AA 🔒 customers.microsoft.com

< > ↗ ↘ ↗ ↘

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

f t in e

September 6, 2022

Print

AA 🔒 customers.microsoft.com

< > ↗ ↘ ↗ ↘

Customer Stories Search

Microsoft

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

Share this story

f t in e

September 6, 2022

Print

AA 🔒 customers.microsoft.com

< > ↗ ↘ ↗ ↘

Storebrand flytter Swift til skyen

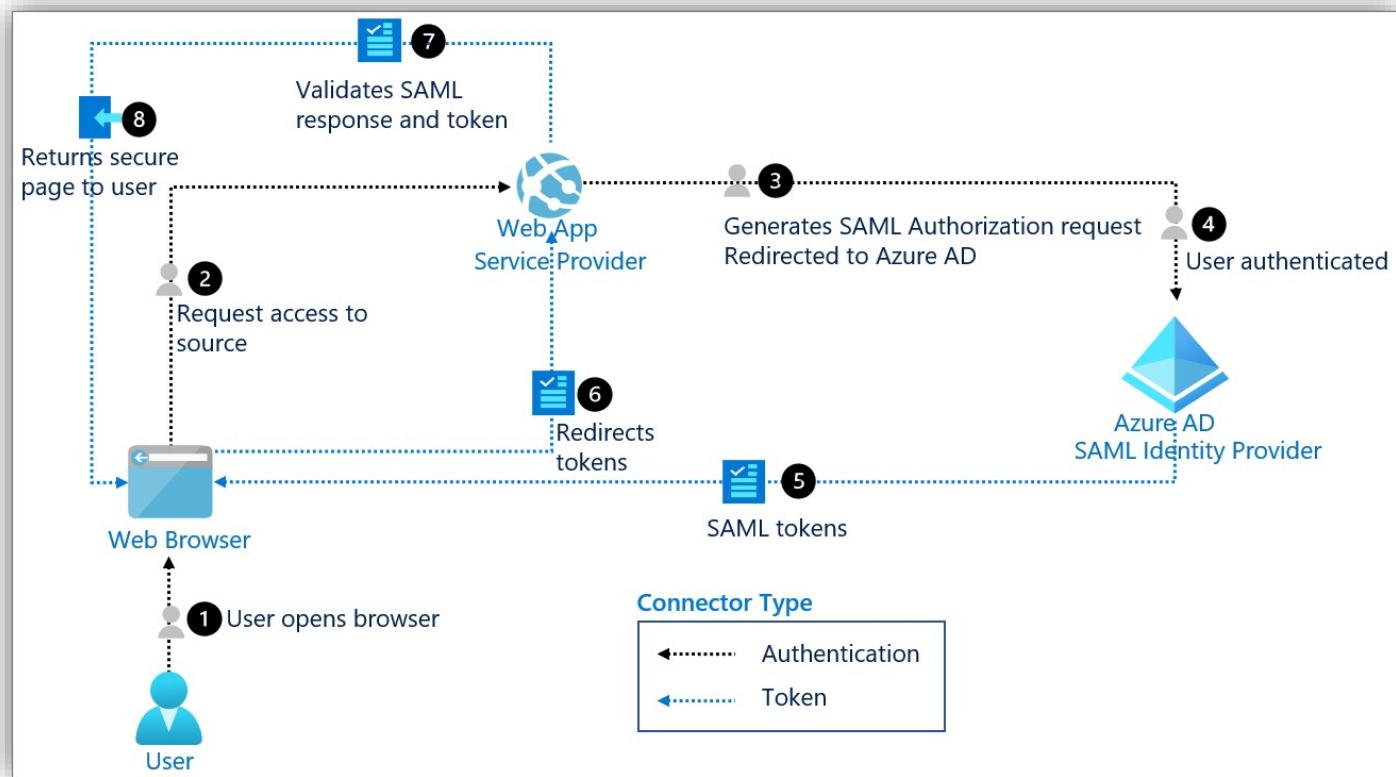
Storebrand migrerer i disse dager infrastrukturen til Swift fra fysiske datasentre til en skybasert løsning.

TRYGGERE: – Vi sparer selvlagt 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

A screenshot of a Microsoft Edge browser window. The address bar shows the URL `login.microsoftonline.com/44b538f1-aeed-4959-a674-24d907b93966/saml2`. The main content is a "Sign in" page for "storebrand". It has a logo, a text input field for "someone@example.com", a "Next" button, and a "Sign-in options" link at the bottom.

The developer tools Network tab is open, showing a request to `https://jira.storebrand.no/plugins/servlet/samlsso`. A red dashed arrow labeled "1" points from this entry to the corresponding entry in the second screenshot's Network tab.

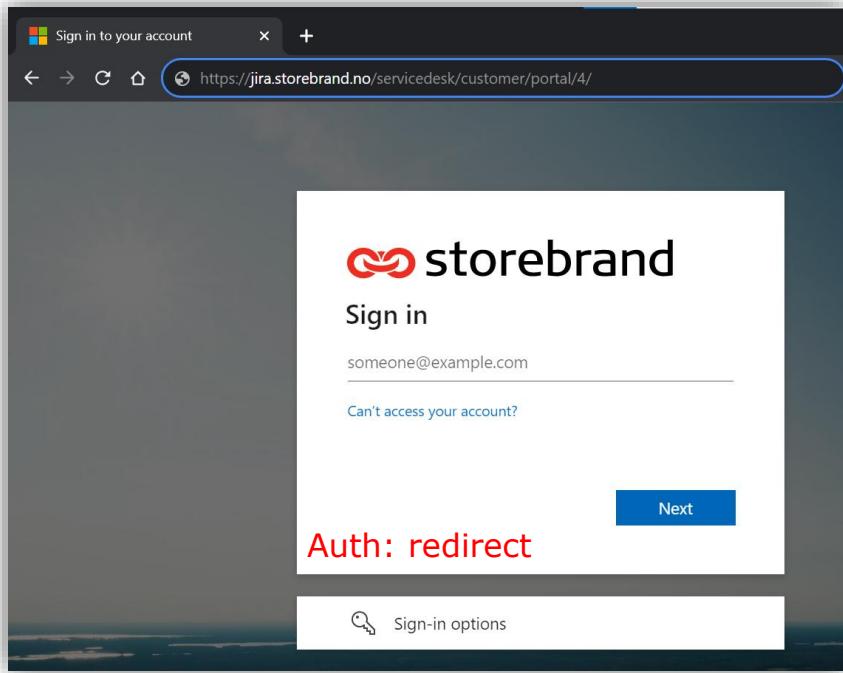
This screenshot shows two separate browser windows or tabs of developer tools, both displaying network requests for Azure AD authentication.

Top Tab (Request 2): Shows a request to `https://jira.storebrand.no/plugins/servlet/samlsso` with a status code of 200 OK. The "General" section shows the request URL and method, and the "Response Headers" section includes `cache-control: no-cache, no-store, must-revalidate` and `content-encoding: gzip`.

Bottom Tab (Request 3): Shows a request to `https://login.microsoftonline.com/44b538f1-aeed-4959-a674-24d907b93966/saml2` with a status code of 200 OK. The "General" section shows the request URL and method, and the "Response Headers" section includes `Cache-Control: no-store, no-cache` and `Content-Encoding: gzip`.

Red dashed arrows labeled "2" and "3" point from the request URLs in the Network tabs to the corresponding entries in the developer tool panes.

SSO and WAF: expected behavior



Two screenshots of 403 Forbidden errors from a Microsoft Azure Application Gateway. Both screenshots have a title "403 Forbidden" and a sub-header "WAF: block". The first screenshot shows the URL jira.storebrand.no/servicedesk/customer/portal/4/user/signup. The second screenshot shows the URL jira.storebrand.no/?jquery=SELECT%20%271%27=%271. Both screenshots include the text "Microsoft-Azure-Application-Gateway/v2" and a red "403 Forbidden" message.

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

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

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 browser is <https://jirastorebrand.no/Issues/?filter=3>. The dialog shows fields for Project (JIRA Support JIRA), Issue Type (Recent Projects: Security (SEC), Cirrus (CIR)), Customer Request Type (All Projects: Cirrus (CIR), GRC (GRC), Security (SEC)), and Summary (empty). A note says "used to create a ticket. This custom field is created programmatically." The Description field has a rich text editor. Buttons at the bottom are "Create another", "Create", and "Cancel".

A screenshot of a Jira 'All issues' search results page. The URL in the browser is <https://www.browserling.com/>. The browser title bar shows "[All issues] Issue Navigator - Jira". The search bar contains "jirastorebrand.no/Issues/?filter=4". The results table has columns for Project, Status, Contains text, and More. The 'All issues' filter is selected. The results section shows a message: "No issues were found to match your search. Try logging in to see more results." There is a cartoon illustration of two people shaking hands.

Anonymous access: create an issue

The image shows a Jira interface with three main sections illustrating the process of creating an issue and viewing it.

Top Left: A screenshot of the "Create Issue" page. It shows fields for "Project" (dropdown menu) and "Issue Type" (set to "User story"). Below these are "Next" and "Cancel" buttons. A red dashed arrow points downwards from this screen towards the bottom center.

Top Right: A screenshot of the issue details page for "Test X". The URL is https://jira.storebrand.no/browse/GRC-948. The issue has a status of "In Progress" and priority "Average". The reporter is listed as "Anonymous". A red dashed arrow points upwards from the "Create Issue" screen towards this one.

Bottom: A screenshot of the "All issues" search results page. The search bar includes filters for "Project: All", "Status: All", and "Contains text". A success message box in the bottom right corner states: "Issue GRC-948 - Test X has been successfully created." A red dashed arrow points upwards from this message box towards the "Create Issue" screen.

Anonymous access: create an issue

The screenshot shows a Jira issue creation page for a task titled "Test X". The "Reported" field is highlighted with a red dashed box, showing the value "Anonymous". Other fields like "Assignee" and "Request participants" also have red dashed boxes around them, indicating they are being reviewed or are part of the anonymous access test.

Issue 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

Drop files to attach, or browse.

Attachments: None

Related knowledge base articles: None

Activity:

- All Comments Work Log History Activity Emails Transitions

There are no comments yet on this issue.

Comments: Click to add comment

SLAs: No SLA set for this issue

People:

- Assignee: Unassigned
- Reported: Anonymous
- Request participants: None
- Votes: 0
- Watchers: 0

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 interface with the following details:

- Search Bar:** Contains filters: GRC, Type: All, Status: All, Assignee: All, Contains text: "Feil Spot-rate", and a Search button.
- Issue List:** Shows three issues:
 - GRC-950: Feil Spot-rate på Auto-FX medfører prisingsavvik på FORNYBAR (20 bp) - Selected, highlighted in blue.
 - GRC-948: Test X
 - GRC-947: Feil faktura registrert på feil person
- Issue Details:** For GRC-950:
 - Title:** Feil Spot-rate på Auto-FX medfører prisingsavvik på FORNYBAR (20 bp)
 - Type:** Task
 - Priority:** None
 - SLAs:** 2d 7h
 - Time to start:** Within 2d 8h
 - Time to done:** 1mo
- Right Panel:** A context menu is open, showing options like Profile, Accessibility, Atlassian Marketplace, MY JIRA HOME, Dashboard, Service project, Boards, Structure, Issue Navigator, Assets, and Log Out.

Impact: brute force

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

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

Password

Remember my login on this computer

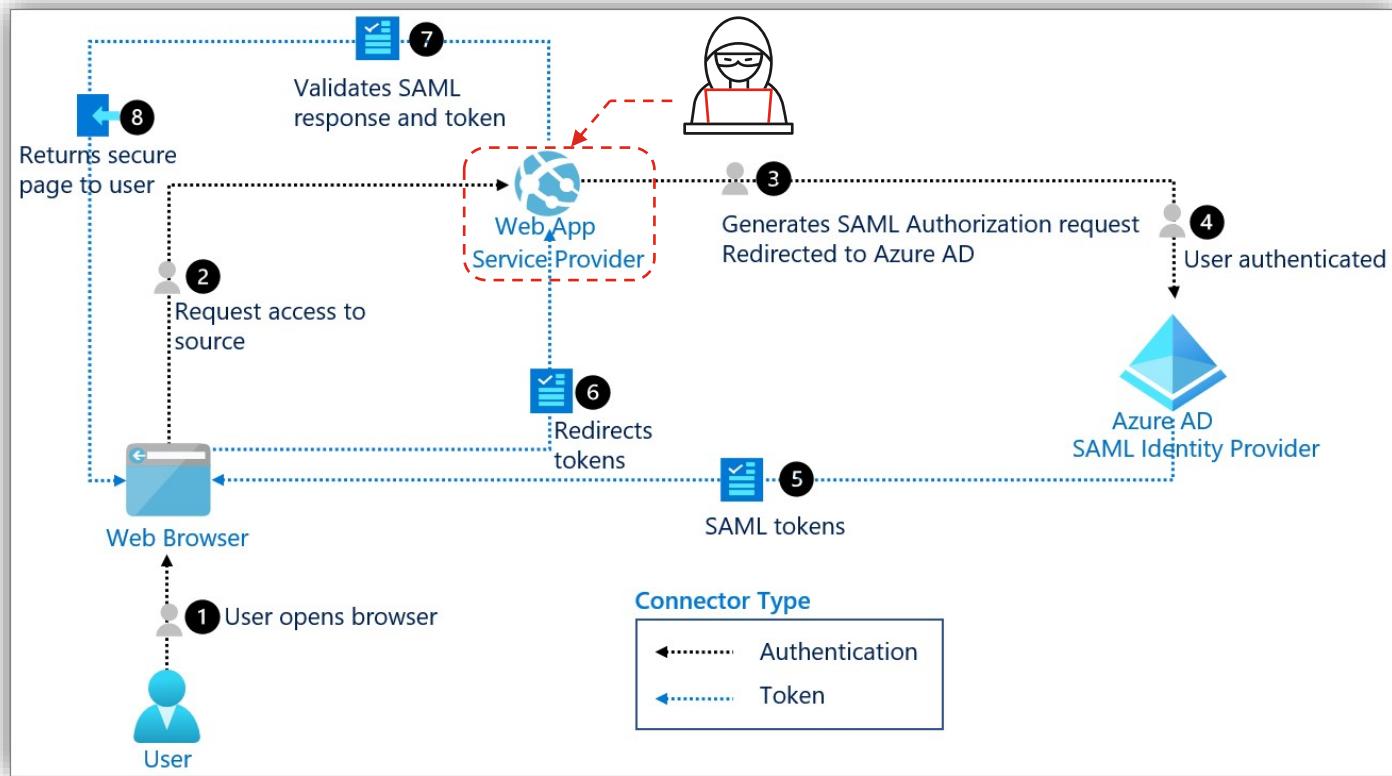
Not a member? To request an account, please contact your Jira administrators.

Log In Can't access your account?

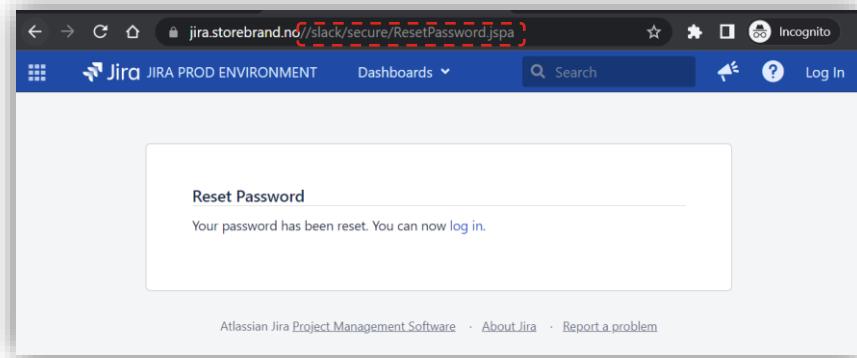
Atlassian Jira Project Management Software · About Jira · Report a problem

ATLASSIAN

SAML authentication with Microsoft Entra ID



Impact: password reset (via Jira)



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])

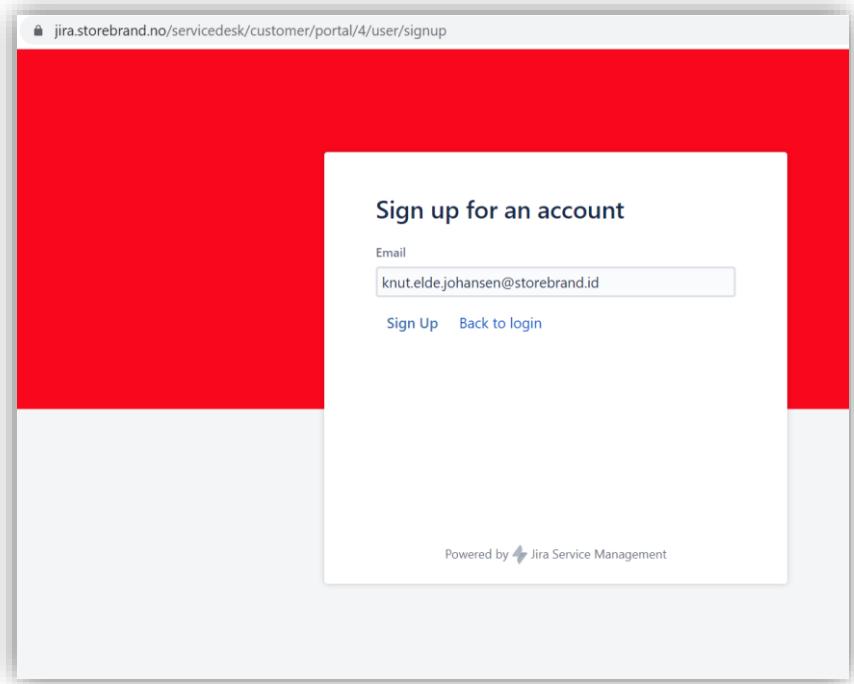
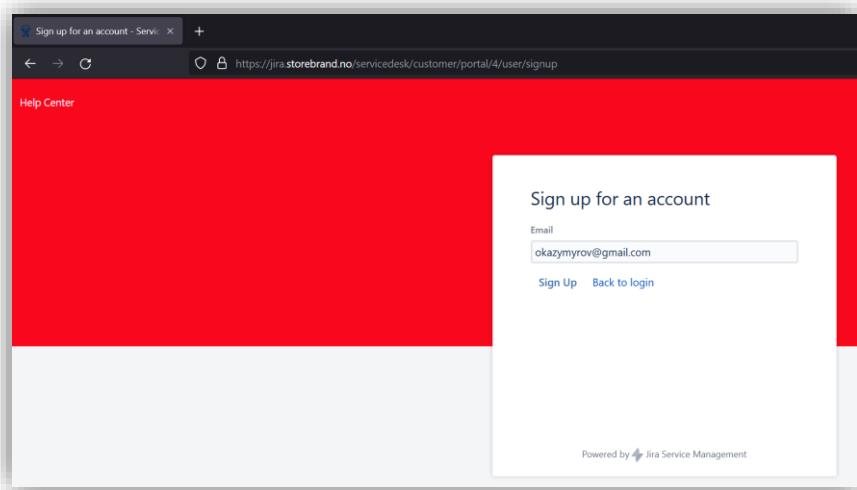
Here are the details of your account:

Username: [REDACTED]

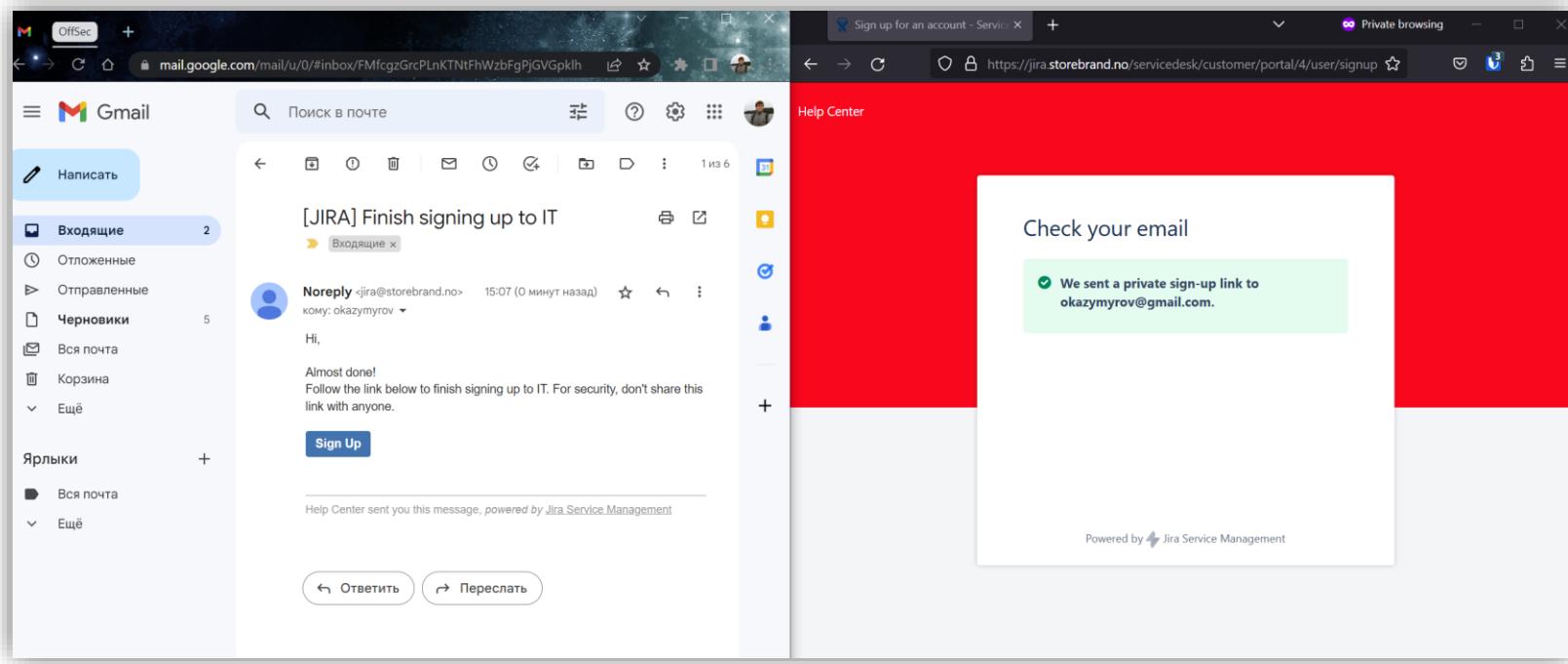
Email: oleksandr.kazymyrov@storebrand.no

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.

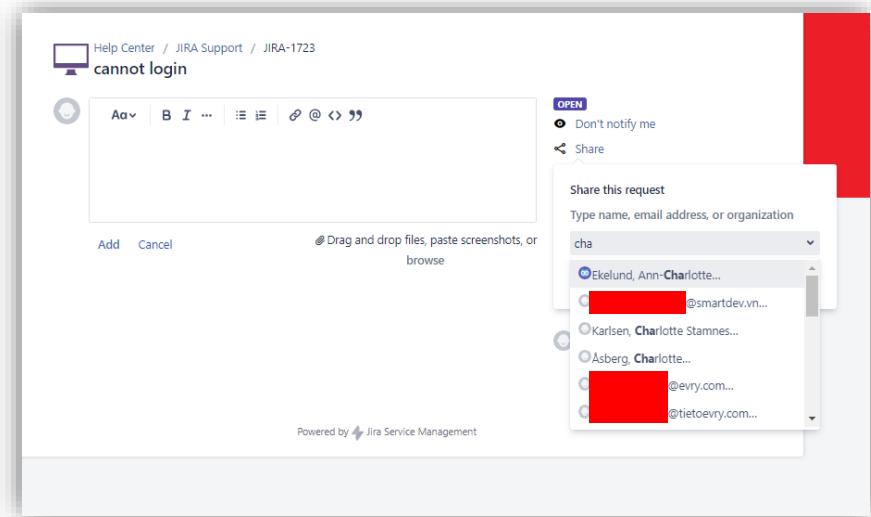
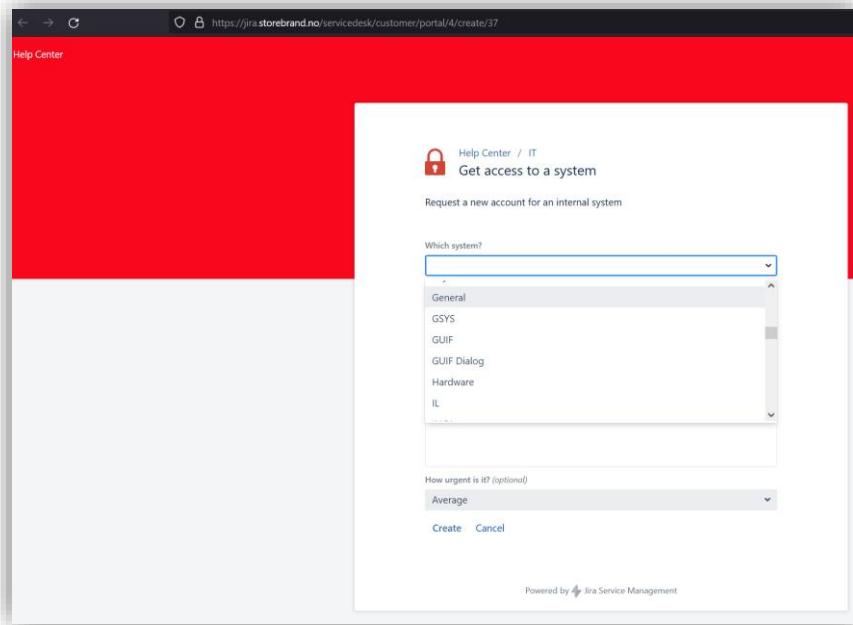
General

CMDB

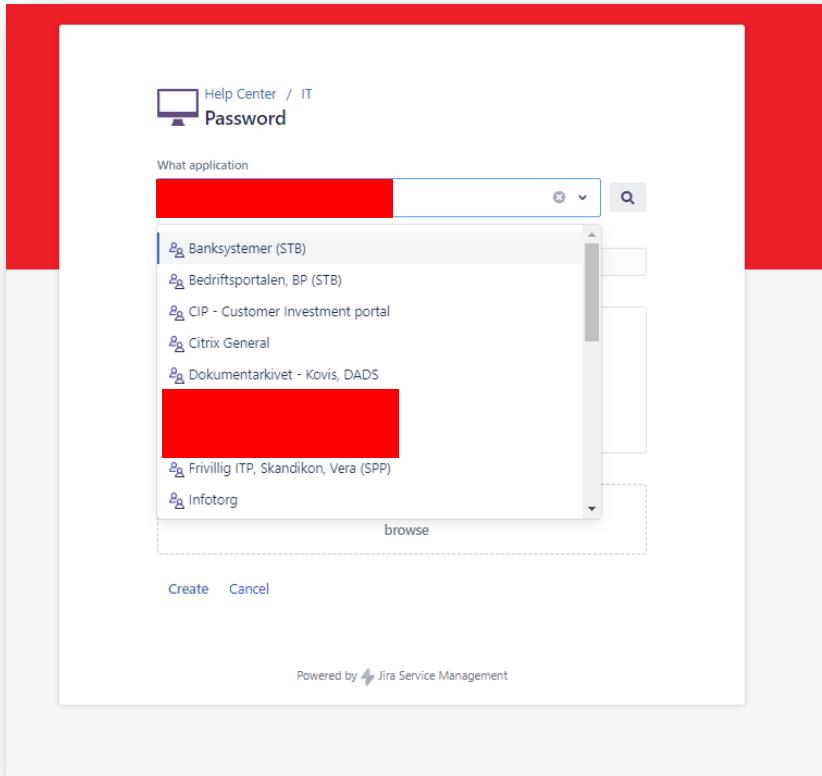
- Register Azure tagging convention for existing application in CMDB
- Register a new application in CMDB

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 details are as follows:

- Type:** Service
- Priority:** Info
- Components/Labs:** the - Printing Automation - NEW
- Description:** Do not disable this account for now please /Kenny
- Attachments:** Drop files to attach, or browse
- SLA:** No SLA set for this issue
- People:** Assignee: Unassigned; Request participant: None; Organizations: None; Votes: None; Watchers: None
- Service project request:** Request type: Information; Customer status: Open; Channel: Portal; View customer request
- Dates:** Created: 1 minute ago; Updated: 1 minute ago
- Development:** Create branch

The screenshot shows the Jira activity feed with the following entry:

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.

Edit · Delete · ⚙

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

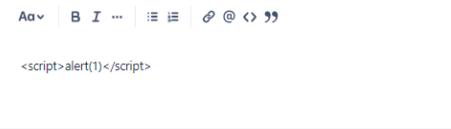
Shared with
 Torsbakken, Stig Tombre
Creator

Impact: social engineering via IT support

Help Center / JIRA Support / JIRA-1723

cannot login

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



OPEN Don't notify me
 Share

Shared with

- FakeUser Creator
- Bergerud, Øyvind Remove
- Torsbakken, Stig Tomre 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 Fl2

ANALYZE Don't notify me
 Share

Comment on this request...

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

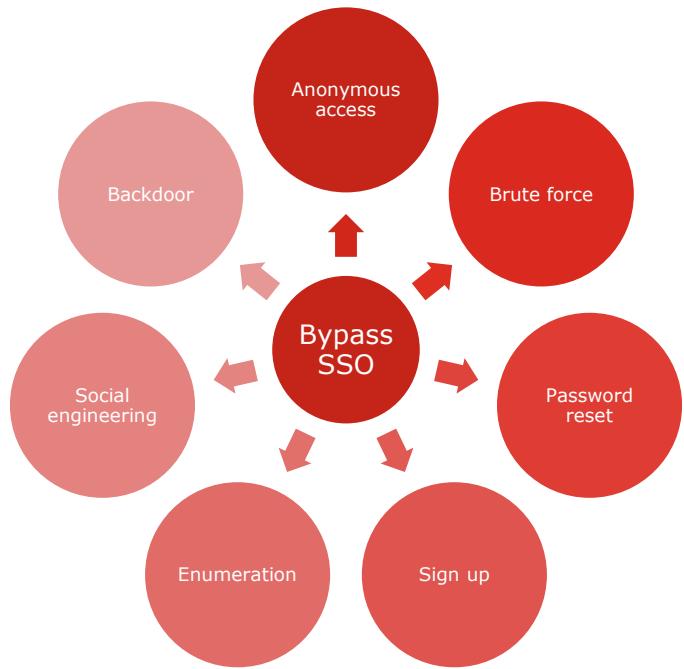
Impact: backdoor

A screenshot of a web browser window showing 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 dialog box is open, titled "Personal Access Tokens". The dialog contains a red dashed box highlighting the text: "Use personal access tokens as a safe alternative to authenticating with username and password. [Learn more.](#)". Below this, a table lists a single token entry:

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

At the bottom of the modal, there are "Close" and "Create token" buttons. The footer of the page shows "(GMT+01:00) Oslo" and "Powered by Jira Service Management".

Summary of impact





”

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

Confucius