TS010217145 - APPSEC - Improper Session Management

Case history

9 Dec 2022

01:17 PM IST **pmr user** (Customer) changed Status from ***Closed by Client*** to ***Closed - Archived***.

9 Nov 2022

01:08 PM IST **pmr user** (Customer) changed Status from ***Waiting for IBM*** to ***Closed by Client***.

01:08 PM IST **pmr user** (Customer)
Hello Mason,
Yes , for now this can be closed
Please push DEV team to work on RFE on priority
Kind Regards,
Swapnil

01:08 PM IST **pmr user** (Customer) changed Status from ***Awaiting your feedback*** to ***Waiting for IBM***.

7 Nov 2022

01:18 PM IST **Zhao.Yu.Ge** (IBM)
Hi Swapnil,
I will inform dev team a RFE is opened for this.
However, support case cannot be used to track RFE. Since this is WAD, would you mind close this case?
Thank you!
Best,
Mason

01:18 PM IST **Zhao.Yu.Ge (https://Zhao.Yu.Ge)** (IBM) changed Status from ***Waiting for IBM*** to ***Awaiting your feedback***.

12:53 PM IST **pmr user** (Customer)
Hello Mason,
We have successfully created the RFE for the same
ESS-I-40
Kind Regards,
Swapnil

12:53 PM IST **pmr user** (Customer) changed Status from ***Awaiting your feedback*** to ***Waiting for IBM***.

18 Oct 2022

12:57 PM IST **Zhao.Yu.Ge** (IBM)
Hi Swapnil,
This is what Dev team explains to me:
This is a WEB interface of IBM storage product which is running locally(intranet) and not exposed to external world (Internet) and this is being used by specific users allocated roles by admin and also provides sudo root privileges them for running mm* commands.

Why he meant by WAD is, It was not intended to work and cover a scenario where user can not login from multiple browsers or even from same IP, meaning a same user can also access the GUI application from two different IPs even if single browser has been used from both the systems.
Having said that, If this has to be covered the there will also need be a handling of use case where one user at one time login from single IP and IP detection while login is not available. So he would like to request you, open a RFE in order to cater these requirements and and even they want product to cover more use cases and based on offering management and priorities.
Best,
Mason

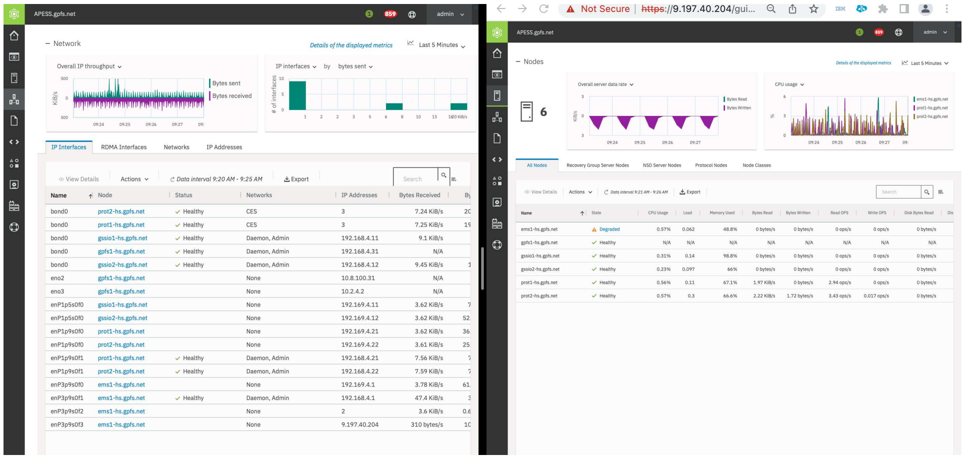
12:57 PM IST **Zhao.Yu.Ge (https://Zhao.Yu.Ge)** (IBM) changed Status from ***Waiting for IBM*** to ***Awaiting your feedback***.

17 Oct 2022

11:45 AM IST **pmr user** (Customer)
Hello Mason,
It is mentioned, the system is designed the way it is behaving. I would presume, this means, system is designed to allow simultaneous logins in the application. If this understanding is correct, could you please provide examples or case studies where it would be required to use the functionality of simultaneous login for the same user.
I am trying to get details so that we can go back to the auditor with the rational on why simultaneous login is required and in case simultaneous login is not allowed, what are the business cases that will stop working
Kind Regards,
Swapnil

11:45 AM IST **pmr user** (Customer) changed Status from ***Awaiting your feedback*** to ***Waiting for IBM***.

07:10 AM IST **Zhao.Yu.Ge** (IBM)
Hi Swapnil,
From my perspective, if one user need to monitor different metrics of the cluster the same time, then two or more GUI interface will be needed.
eg. You may want to monitor CPU/Memory usage and network throughput at the same time from GUI when the cluster is handling large workload. To achieve this, two GUI interface will be needed in two browsers(In example below, two GUI opened in Safari and Chrome respectively).



Name	Node	Status	Networks	IP Addresses	Bytes Received	By
bond0	prot2-hs.gpfs.net	✓ Healthy	CES	3	7.24 KiB/s	20
bond0	prot1-hs.gpfs.net	✓ Healthy	CES	3	7.25 KiB/s	19
bond0	gssio1-hs.gpfs.net	✓ Healthy	Daemon, Admin	192.168.4.11	9.1 KiB/s	
bond0	gpfs1-hs.gpfs.net	✓ Healthy	Daemon, Admin	192.168.4.31	N/A	
bond0	gssio2-hs.gpfs.net	✓ Healthy	Daemon, Admin	192.168.4.12	9.45 KiB/s	1
eno2	gpfs1-hs.gpfs.net		None	10.8.100.31	N/A	
eno3	gpfs1-hs.gpfs.net		None	10.2.4.2	N/A	
enP1p5s0f0	gssio1-hs.gpfs.net		None	192.169.4.11	3.62 KiB/s	7
enP1p5s0f0	gssio2-hs.gpfs.net		None	192.169.4.12	3.62 KiB/s	52.
enP1p9s0f0	prot1-hs.gpfs.net		None	192.169.4.21	3.62 KiB/s	36.
enP1p9s0f0	prot2-hs.gpfs.net		None	192.169.4.22	3.61 KiB/s	25.
enP1p9s0f1	prot1-hs.gpfs.net	✓ Healthy	Daemon, Admin	192.168.4.21	7.56 KiB/s	7
enP1p9s0f1	prot2-hs.gpfs.net	✓ Healthy	Daemon, Admin	192.168.4.22	7.59 KiB/s	7
enP3p9s0f0	ems1-hs.gpfs.net		None	192.169.4.1	3.78 KiB/s	61.
enP3p9s0f1	ems1-hs.gpfs.net	✓ Healthy	Daemon, Admin	192.168.4.1	47.4 KiB/s	3
enP3p9s0f2	ems1-hs.gpfs.net		None	2	3.6 KiB/s	0.6
enP3p9s0f3	ems1-hs.gpfs.net		None	9.197.40.204	310 bytes/s	10

Name	State	CPU Usage	Load	Memory Used	Bytes Read	Bytes Written	Read OPS	Write OPS	Disk Bytes Read	Dis
ems1-hs.gpfs.net	⚠ Degraded	0.57%	0.062	48.8%	0 bytes/s	0 bytes/s	0 ops/s	0 ops/s	0 bytes/s	
gpfs1-hs.gpfs.net	✓ Healthy	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
gssio1-hs.gpfs.net	✓ Healthy	0.31%	0.14	98.8%	0 bytes/s	0 bytes/s	0 ops/s	0 ops/s	0 bytes/s	
gssio2-hs.gpfs.net	✓ Healthy	0.23%	0.097	66%	0 bytes/s	0 bytes/s	0 ops/s	0 ops/s	0 bytes/s	
prot1-hs.gpfs.net	✓ Healthy	0.56%	0.11	67.1%	1.97 KiB/s	0 bytes/s	2.94 ops/s	0 ops/s	0 bytes/s	
prot2-hs.gpfs.net	✓ Healthy	0.57%	0.3	66.6%	2.22 KiB/s	1.72 bytes/s	3.43 ops/s	0.017 ops/s	0 bytes/s	

I've also forwarded your concern to dev team, let's expect their opinion too. Besides, dev team believe your request is valid but is a completely new design. I suppose they will prioritize your code enhancement request if you open a RFE.
Thank you!
Best,
Mason

07:10 AM IST **[Zhao.Yu.Ge (https://Zhao.Yu.Ge)](https://Zhao.Yu.Ge)** (IBM) changed Status from ***Waiting for IBM*** to ***Awaiting your feedback***.

---

13 Oct 2022

02:27 PM IST **pmr user** (Customer)
Hello Mason,
What are the legitimate business cases to allow the user to have simultaneous session?
In other words, if simultaneous session are blocks what, what are the business use cases will fail and how
Kind Regards,
Swapnil

02:27 PM IST **pmr user** (Customer) changed Status from ***Awaiting your feedback*** to ***Waiting for IBM***.

01:45 PM IST **Zhao.Yu.Ge** (IBM)
Hi Swapnil,

Session Management (Simultaneous session) :

Dev team has confirmed this is worked as designed where the same legitimate user can login to application through different browsers with completely different session. It's completely a design change to realize your request. Dev team expect you to raise this through RFE process and they will prioritize this for future releases.

You can submit your request as a RFE([https://www.ibm.com/developerworks/rfe/ (https://www.ibm.com/developerworks/rfe/)](https://www.ibm.com/developerworks/rfe/)). However, RFE will be assessed first and is not 100 percent guaranteed to be realized in future Spectrum Scale release. RFE is also out of support scope and this case can not be used for tracking RFE.

Let me know if anything is unclear.

Best,
Mason

01:45 PM IST **[Zhao.Yu.Ge (https://Zhao.Yu.Ge)](https://Zhao.Yu.Ge)** (IBM) changed Status from ***IBM is working*** to ***Awaiting your feedback***.

12:08 PM IST **Zhao.Yu.Ge** (IBM)
Hi Swapnil,
Your concern is acknowledged, I will forward it to DEV.
I will keep you posted.
Thank you!
Best,
Mason

12:08 PM IST **[Zhao.Yu.Ge (https://Zhao.Yu.Ge)](https://Zhao.Yu.Ge)** (IBM) changed Status from ***Waiting for IBM*** to ***IBM is working***.

11:50 AM IST **pmr user** (Customer)
Hello Mason,
Improper session management has 2 subsection
1)Session Timeout – This has been resolved when the session timeout changed to 5 mins
However , we need to work on below point
2) Simultaneous session – This issue is related to same user opening multiple sessions either with different browsers and different system. Ideally, the application should allow only one active session per user.
Kind Regards,
Swapnil

11:50 AM IST **pmr user** (Customer) changed Status from ***Awaiting your feedback*** to ***Waiting for IBM***.

---

19 Sep 2022

03:26 PM IST **Zhao.Yu.Ge** (IBM)
Hi team,
No problem, I will wait for clients' response.
BR,
Mason

03:26 PM IST **Zhao.Yu.Ge (https://Zhao.Yu.Ge)** (IBM) changed Status from ***Waiting for IBM*** to ***Awaiting your feedback***.

02:12 PM IST **pmr user** (Customer)
Hello Mason,
Thanks for suggestion .
We have changed session timeout parameter to 5 min and sending this as evidence to reviewer .
Will update you shortly on this
Kind Regards,
Swapnil

---

14 Sep 2022

02:20 PM IST **Zhao.Yu.Ge** (IBM)
Hi team,
I believe the primary concern of yours is that the Spectrum Scale will not auto-logout the current inactive GUI user in certain amount of time(in your case, 21 minutes) and simultaneous login in different browser.
For auto-logout, Spectrum Scale GUI has auto logout feature with default timeout as 5 mins and can be configured to any limit. (Services > GUI > Preferences).
For simultaneous login in different browser, since GUI retain user session for limited time(default 5 mins) so within this range valid user can have multiple tabs open in browser which sometimes you are using else, which means if you open another tab in the same browser then it will automatically routes you to GUI home page. However, if you wanna open the same GUI on another browser then it will create another session in that browser.
In different web browser the session is not identical.
Let me know if you have any other concern.
Thank you!
Best,
Mason
IBM ESS Solution Support
https://www.ibm.com/mysupport (https://www.ibm.com/mysupport)

---

13 Sep 2022

09:54 AM IST **Zhao.Yu.Ge** (IBM)

Hi team,
Spectrum Scale GUI is running local to its cluster i.e. running at localhost and not exposed to external world. It used encrypted HTTPS using SSL V2/V3 which makes it safe from MITM (Man-in-the-middle attack).
Few of cookies used in application are session cookies so they only expires when session gets terminated (e.g. JSESSIONID, _auth). On the other hand other cookies have expiry time (e.g _currentClusterID,userHash etc.).
JSESSIONID is a cookie which is being used by GUI which changes per user session dynamically and _auth is the cookie which frequently gets updated using Session manager which cleans up olders keys (tickets) in the interval of minute and also invalidats during running user session.
Having said that, even if intruder is able to steal the cookies used in Scale GUI then it will not harm an application unless any other network vector has been injected on client infrastructure.
Let me know if you have any other concern.
Thank you!
Best,
Mason
IBM ESS Solution Support
https://www.ibm.com/mysupport (https://www.ibm.com/mysupport)

---

18 Aug 2022

02:06 PM IST **Zhao.Yu.Ge** (IBM)

Hi Subhrendu,
Thank you for your update, I will keep you posted.
BR,
Mason

12:27 PM IST **pmr user** (Customer)

Hi
This issue is raised as part of security review by Deloitte. IBM is implementing solution and Deloitte is security reviewer.
The issue raised by Deloitte is as below:
"An attacker can get the user session cookies by any means Session Spoofer, Cookie Stealer etc. As the user cookies are not expiring so an attacker can directly inject the stolen cookies of a victim in a request from browser and thus can have access to the victims account."
Recommendation by Deloitte: "Do not expose session ID in the URL: Session IDs should not be exposed in the URL (e.g., URL rewriting).
Session IDs should timeout: User sessions or authentication tokens should be properly invalidated during logout.
Recreate session IDs: Session IDs should be recreated after successful login.
Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session IDs should not be in the URL, be securely stored and invalidated after logout, idle, and absolute timeouts."
Please refer to attachment for details.
Regards
Subhrendu K Biswas

---

16 Aug 2022

12:34 PM IST **Zhao.Yu.Ge** (IBM)
Hi team,
Since we have not heard back from you, we will close this case in 48hrs. At any time in the next 30 days you may re-open this case using the button at the top of your case screen.
Thank you!
Best,
Mason
IBM ESS Solution Support
https://www.ibm.com/mysupport (https://www.ibm.com/mysupport)

12 Aug 2022

12:42 PM IST **Zhao.Yu.Ge** (IBM)
Hi team,
Could you please give us more detailed information about this case?
Thank you!
Best,
Mason
IBM ESS Solution Support
https://www.ibm.com/mysupport (https://www.ibm.com/mysupport)

9 Aug 2022

06:47 AM IST **Zhao.Yu.Ge** (IBM)
Hi team,
IBM Support is reviewing the case. Future updates will be viewable here.
Could you please give us more detailed information about "**In APPSEC review it has identified as Improper Session Management**?"
For additional help using our site, refer to the “Documentation” drop down found at the top of the Support site. https://www.ibm.com/mysupport (https://www.ibm.com/mysupport)
Best,
Mason
IBM ESS Solution Support
https://www.ibm.com/mysupport (https://www.ibm.com/mysupport)

8 Aug 2022

04:22 PM IST **pmr user** (Customer) created this case