Sent Time: 2016-04-15 14:39:57 GMT-04:00(Eastern Daylight Time)
From: "Dana [redacted]
To: Leonard Small [redacted], "Marc [redacted]
Subject: FW: EDG/AED Security Concern (RE: OSB Libraries)
Attachments: 'smime.p7s', 'smime.p7s', 'smime.p7s', 'smime.p7s', 'smime.p7s', 'smime.p7s'

Classification: ~~SECRET//~~[redacted]~~/NOFORN~~

[redacted]
==

Marc/Leonard:

Per our discussion earlier today. I spoke to Anthony Leonis this afternoon - the Administrative access re-initiation was not a simple click and play. It was a deliberate command to server – to allow Administrative access. By the way…these systems are related to operational [redacted] efforts. I fully concur with Anthony's concerns.

Let me know if you need anything else – will stand by. I'll brief Michele [redacted] – advise her simply "…we have passed the information from EDG, and waiting for SIB response."

Have a good weekend.

Dana

From: Anthony Leonis
Sent: Friday, April 15, 2016 2:06 PM
To: Dana [redacted] Susan [redacted]
Michele [redacted]
Cc: Anthony Leonis [redacted]; Michael [redacted] S[redacted]; Karen [redacted]
Subject: EDG/AED Security Concern (RE: OSB Libraries)

Classification: ~~SECRET//~~[redacted]~~/NOFORN~~

[redacted]
==

Hi Dana, Susan, Michele --

GOVERNMENT
EXHIBIT
1062
S2 17 Cr. 548 (PAC)

(~~S//~~[redacted]~~/NF~~) I have included the email below from Jeremy Weber and a verification from Sean [redacted] on what they said to provide a direct account of the information I'm summarizing below. In addition, I've provided some emails as reference material having to deal with the movement of Joshua to another branch in EDG/AED. If you have questions, please let me know.

****

(~~S//~~[redacted]~~/NF~~) At the end of March 2016, EDG/AED/OSB staff were directed by EDG and CCI management to ensure that all OSB projects were properly resourced, all OSB-related development resources (to include computer network exploitation (CNE) related code libraries, development tools, etc.) were accessed by the appropriate people in OSB, and any projects that were not going to remain in OSB be moved to the appropriate EDG branch immediately. This move was made following a personnel situation that occurred in March 2016 – reference attached emails relating to "Office Moves." (Note: AED/OSB is responsible for developing, among other things, [redacted] tools used [redacted] to acquire data from targeted systems [redacted])

(~~S//NF~~) On Thursday, 14 April, as part of this process, OSB administrators of OSB's CNE Code Component Libraries (OSB Libraries) removed Joshua Schulte's administrative access to the OSB's component code libraries because he was moved from AED/OSB to AED/RDB at the end of March 2016 (ref. attached emails). This action was taken in direct response to the direction provided by EDG and CCI management at the end of March 2016. In doing so, OSB Administrators of the OSB Libraries removed Joshua's administrative access to the library, but enabled him to maintain user-based access to the code repository / server to permit him to access code in the library and commit code to the library through the normal peer review process (ref. the emails listed below).

(U//~~AIUO~~) After interviewing multiple sources (ref. the email conversation material below), the following information was learned:

1) (~~S//NF~~) Prior to his move from AED/OSB to AED/RDB, on several occasions Joshua used his administrative accesses to the code base to check out and commit CNE-related code changes to the OSB code libraries without following the prescribed peer review process. As a result of these actionsand on some occasions due to the lack of a code peer review, the non-peer reviewed committed code did not compile and/or caused subsequent component users to redevelop and resubmit the code to ensure that follow-on users would not experience the same problems. This behavior caused several man-hours of re-work on these non-peer reviewed components, and resulted in other AED/OSB developers to speak with Joshua verbally and request on several occasions that he stop the behavior.

2) (~~C//NF~~) Upon learning that he was removed as an administrator of the OSB Libraries on 14 April 2016, Joshua met with Jeremy Weber (one of the OSB Library Admins) and Sean [redacted] (AED/OSB Branch Chief) to discuss the situation. At the conclusion of the final discussion with

Jeremy Weber , where Jeremy explained to Joshua that Joshua remarked to Jeremy, Joshua "… will eventually get access back to the libraries and that access should just be enabled now …." (ref. the emails below)

3) (~~S//NF~~) After the discussion and emails sent on the topic (ref. the emails below), before the end of the day on 14 April 2016 Jeremy checked the accesses on the OSB code library server and discovered that Joshua re-instituted his administrative access to the server via other administrative rights Joshua possessed on EDG's DEVLan system.

(U//~~AIUO~~) These actions (as well as others listed and attached to this email) are very concerning for many reasons:

(U//~~AIUO~~) First, in any IT environment, Administrative Rights are provided to trusted individuals for the sole purpose of ensuring that the right people have access to data in order to complete tasks related to their job. As detailed explicitly in the Agency's annual AISC trainings, (from AISC 2016, Module 2: User Accounts) "…The Agency has strict regulations and procedures for granting access to IT systems and managing user accounts. Careful management of user accounts is necessary to ensure only legitimate, trusted individuals have access…. References: AR 9-38, AR 9-25." As such, those who have rights to any system are to be reviewed, esp. as a person changes job duties. Additionally, after a change of access is reviewed and action is taken, by no means is the individual who's accesses were adjusted allowed and/or permitted to attempt or renew their previous authorizations to any particular system. This is a direct violation of trust, and a violation of Agency policy.

(~~S//~~[redacted]~~/NF~~) Furthermore, given that EDG's DevLan system and any code bases connected to it contain some of the CIA [redacted] most protected technical secrets enabling the Agency [redacted] conduct CNE-related activities [redacted], administrative accesses were provided to individuals with the main purpose of enabling the mission – and these rights were granted based on trust with the goal of ensuring that individuals protect this intellectual property and the capabilities stored on these systems, and not use the administrative rights / accesses to promote personal goals or provide control over components for individual gain. Violation of this trust is a serious matter – as EDG's and the CCI's operational model requires that all individuals can be trusted to maintain a level of professionalism and understand their roles, without putting personal objectives ahead of the mission.

(~~S//~~[redacted]~~/NF~~) As a result, Joshua's direct insistence that he maintain access, using language indicating that he would find a way to ensure this access is maintained regardless of management's decision to remove his access, and willingness to act to re-institute his administrative access to a system that he should not have these rights must be taken seriously. This is in direct violation of Agency policy, and raises concerns whether Joshua should be permitted continued access EDG's code bases in the future. EDG's development model relies on very talented individuals across the country coming up with technical solutions to some of the toughest cyber problems… but it also relies entirely on the fact that all individuals can be trusted to protect EDG, CCI, Agency and IC equities by following the security models with the appropriate accesses in place to protect us all. Failure to do so puts our entire set of cyber tools – [redacted] and those using them [redacted] – at risk for years to come.

If you need additional information, please contact me – happy to assist in any means necessary,
Anthony

From: Sean [redacted]
Sent: Friday, April 15, 2016 1:50 PM
To: Anthony Leonis [redacted]
Subject: RE: OSB Libraries.

Classification: ~~SECRET~~

[redacted]
===

I had a discussion with Josh yesterday as to the status of his involvement in the OSB libraries. He indicated that he was told that he would no longer be part of the library initiative, but was confused because he thought he would be able to continue working the projects with which he was involved. I told him we wanted to make sure that OSB projects stayed in OSB, and RDB projects remained in RDB, and that was the reason we decided to transfer the 2 official projects he was working on to RDB control. I told him we never specifically discussed the libraries, but that it was my impression that anyone could contribute to the initiative and that he would just need to work with Jeremy and Frank to get new code incorporated into the library repository. At no/no time during the conversation did we discuss administrator access (or any access permissions for that matter) to the database. It was a short conversation centered more around the fact that Josh would still be able to use and contribute to the library initiative.

After he left my office, he went to discuss the libraries with Jeremy. I was informed by Jeremy later that Josh had stated that I said it would be fine to re-add him to the administrator group. I told Jeremy that was not accurate, shared with him the gist of our conversation, and told him he should send a note to Anthony and Brent about the request. At some point soon after, Jeremy discovered that access permissions had been altered, and included that information in the note that was ultimately drafted last night.

From: Anthony Leonis
Sent: Friday, April 15, 2016 1:15 PM
To: Sean [redacted]
Cc: Anthony Leonis [redacted]
Subject: RE: OSB Libraries.
Importance: High

Classification: ~~SECRET~~

[redacted]

==

Hi Sean –

Please confirm the direction you provided to Joshua in regards to the highlighted statements from Jeremy Weber below:

“Josh and I did have a conversation yesterday (14 April 2016), he came up after finding that he no longer had permissions to merge into the long lived branches and wanted to know why this was the case and whose decision it had been. I informed him that this was a decision that Sean had made, and that I agreed with the decision. I stated that since Josh was no longer a member of OSB, and since the libraries were still an OSB project, he should not have the authority to merge into the long lived branches. He disagreed with this answer, and stated that when he agreed to move to RDB that it was with the understanding that he would keep all his projects. In his view the libraries were his idea that he should remain in charge of them. I informed him that my understanding of the situation was different and he could talk to Sean about it which he did. After a long discussion with Sean he returned to my desk and said that Sean stated that it was ok for him to have admin access to the libraries, and that I should re-enable his access, to which I replied that I would discuss with Sean. Schulte then finished the conversation by stating that he “will eventually get access back to the libraries and that access should just be enabled now”. I took this statement as him just saying he was going to win the argument and I shouldn’t bother pushing back. After he departed, I discussed things with Sean where it was affirmed that the ok to give admin access to Schulte was not a thing, and that I should e-mail Schulte the specifics of his role (see the e-mail sent last night). Following sending the e-mail, and reading his response I took a look at the audit logs on the libraries themselves. The logs showed that Schulte had re-enabled his direct write access to Master and Develop shortly after sending a response to my e-mail detailing his responsibilities. Again, the only reason to have access to Master and Develop is to control what is able to be merged into the libraries. Not having access to these branches in no way limits being able to contribute to / use the libraries.”

Thanks,
Anthony

From: Jeremy Weber
Sent: Friday, April 15, 2016 12:12 PM
To: Anthony Leonis [redacted]; Sean [redacted] Richard [redacted]
Subject: RE: OSB Libraries.

Classification: ~~SECRET~~

[redacted]
===

Sorry for the spam, because of the below the classification on this e-mail should be bumped up to Secret.

--
Jeremy

Anthony

First, I’ll provide some background in regards to the OSB libraries. This is an undertaking I started two years ago because OSB (specifically myself, Frank Stedman, Matt and Schulte) felt that it was fighting a losing battle in regards to QRCs. With rise in difficulty of CNE operations, both in terms of [redacted] and general tradecraft guidelines it was decided that it was no longer realistic to write new code under the average QRC timeline and have it meet CIA standards of quality. Furthermore, we were cognizant of the fact that we were copying and pasting code from one project to another without any method of tracking who was using what and what tools shared [redacted] The best example of this is our old [redacted] survey. This used to be the go to survey for OSB whenever the requirement needed basic computer information. Without specific numbers to back things up, I would say that [redacted] tools written by OSB had this code embedded, and I would be surprised if there were any developers in OSB who hadn’t used it. The [redacted] issue is obvious, but we also realized that everyone had their own tweaked version of [redacted] survey that fixed a bug that was found but we would never share with other developers so they could improve their projects. This is the reason the OSB libraries were born.

We had three goals:

1. Provide tested, ready to go, code to cover the majority of our requirements.
2. Provide a process in which all developers could contribute and learn from code being written for said libraries.
3. Provide a means for us to track what code is being used where.

To meet these goals we came up with the following plan:

•€€€€€€€€ Libraries would be broken into the specific components of a typical CNE operation

o **CoreLib** – Contains interfaces, and code [redacted] [redacted] which are needed across the board

o **Buffers** – Memory management classes [redacted]

o **Data Transfer** – Means of storing and transmitting collected data

o **Execution Vectors** – Ways to gain initial execution for a process

o **File Collection** – [redacted] prioritize what files need to be collected from disk

o **Miscellaneous –** General techniques which don't necessarily fall under any of the other categories

o **Payload Deployment –** Launching [redacted] [redacted] payload after initial execution

o **Persistence –** Methods to survive power cycles, etc.

o **Privilege Escalation –** Get into a closer ring of an OS's security model

o **Survey –** Gather general information about a target machine

o **System Monitoring and Manipulation –** Methods to catch, suppress, or modify system events

•€€€€€€€€ The libraries would have two controlled 'long lived' branches deemed Master and Develop.

o Master – Officially blessed code, i.e. 1.0, 1.1, 1.2 etc.

o Develop – Stable code that just hasn't been officially blessed yet.

•€€€€€€€€ Writes to Master and Develop would be strictly limited.

o Only a select group of officers could merge code into said branches

o Code could only be merged once it followed a strict pull request process.

•€€€€€€€€ All development would occur in short lived feature branches

o Everyone in AED would have the ability to contribute to the libraries via these feature branches

o All features needed to meet a minimum testing and documentation requirement before being deemed complete

•€€€€€€€€ Once a developer felt a feature was complete they would request it be merged into Develop via a pull request which would initiate a code review

o Fellow developers would review the newly written code for quality and usability.

o At least two developers must approve any pull request.

o Once a minimum level of approval is met, one of the library maintainers can merge the code into develop.

§ Before doing so we validate that proper tests are written, all tests pass or failures are acknowledged, and that everything is properly documented.
•€€€€€€€€ Once develop is deemed far enough along to up the library version the library maintainers merge it into Master

Originally, we identified a single POC for each of the libraries (essentially a library was assigned to each member of OSB), and that POC would be the keeper of Develop. Matt, Josh, and I would be the keepers of Master for everything. We quickly realized that this process didn't work, and it was decided that I would oversee the libraries and Matt, Josh, Frank Stedman, and I would be the keepers for all the long lived branches. I will also point out that despite having direct access to these branches, the library maintainers were still required to follow the pull request model above.

Hopefully that is enough of a background. Now on to your specific questions.

1) The libraries are currently an OSB owned product. We have a desire to make them an AED and have begun talking with Kevin [redacted] to see if we can transfer ownership to him so that it can be an AED level product. However, anyone is free to contribute / use the libraries as they desire, the only thing OSB controls is the keys to Develop and Master.
2) Josh used to have the ability to merge items into Develop and Master. He didn't always follow the process and ended up making more work for Frank Stedman pretty often due to this disregard to the pull request model. His defense was always they were "admin" changes and not new code. I want to make clear that we did not limit his ability to contribute to the libraries, that is still something he can do. All we did was remove his ability to merge changes into the long lived branches, thus removing his ability to control what goes into the official versions.
3) Josh and I did have a conversation yesterday (14 April 2016), he came up after finding that he no longer had permissions to merge into the long lived branches and wanted to know why this was the case and whose decision it had been. I informed him that this was a decision that Sean had made, and that I agreed with the decision. I stated that since Josh was no longer a member of OSB, and since the libraries were still an OSB project, he should not have the authority to merge into the long lived branches. He disagreed with this answer, and stated that when he agreed to move to RDB that it was with the understanding that he would keep all his projects. In his view the libraries were his idea that he should remain in charge of them. I informed him that my understanding of the situation was different and he could talk to Sean about it which he did. After a long discussion with Sean he returned to my desk and said that Sean stated that it was ok for him to have admin access to the libraries, and that I should re-enable his access, to which I replied that I would discuss with Sean. Schulte then finished the conversation by stating that he "will eventually get access back to the libraries and that access should just be enabled now". I took this statement as him just saying he was going to win the argument and I shouldn't bother pushing back. After he departed, I discussed things with Sean where it was affirmed that the ok to give admin access to Schulte was not a thing, and that I should e-mail Schulte the specifics of his role (see the e-mail sent last night). Following sending the e-mail, and reading his response I took a look at the audit logs on the libraries themselves. The logs showed that Schulte had re-enabled

his direct write access to Master and Develop shortly after sending a response to my e-mail detailing his responsibilities. Again, the only reason to have access to Master and Develop is to control what is able to be merged into the libraries. Not having access to these branches in no way limits being able to contribute to / use the libraries.

I hope this answers any questions you have
--
Jeremy

From: Anthony Leonis
Sent: Friday, April 15, 2016 7:29 AM
To: Jeremy Weber [redacted]; Sean [redacted] Richard [redacted]
Cc: Anthony Leonis [redacted]
Subject: RE: OSB Libraries.

```
Classification: UNCLASSIFIED/~~/AIUO~~
=======================================================
```

Ok… I need a little more background to better understand this situation…

Three questions:
1) Are the OSB libraries an entirely-owned OSB product – meaning, if you aren't in OSB you can't generate and/or use the components / libraries?
2) What were Josh's permissions on these products? Is this is a case of someone wanting to have access / contribute or a case of someone wanting control?
3) You mentioned you spoke to Josh about this… was it the email or was there more in person? If there was more in person, I need to better understand the conversation (what was said, etc.)

My concern here is that if Josh wants to use the libraries, and no longer has access to them… that's one thing.
On the other hand, if he changed his permissions to enable him to administer the libraries… that's another.

As did Debra [redacted], I want JoJo to actively look at all EDG libraries. But, in this matter, I urge caution.
If you see anything concerning, please let me know.

Thanks,
Anthony

From: Jeremy Weber [redacted]
Sent: Thursday, April 14, 2016 4:40 PM
To: Anthony Leonis [redacted]; Sean [redacted] Richard [redacted]
[redacted]
Subject: OSB Libraries.

```
Classification: UNCLASSIFIED//~~/AIUO~~
==========================================================
```

Anthony

We have a situation with the libraries and the Atlassian products in general. After we talked with Josh, and I sent the e-mail saying that he doesn't have direct access to our two main branches, he went and modified the permissions to the project to return his previous rights. He is able to do this because he is one of the Atlassian administrators, and I think we need to remove him from this group. I can explain the situation further, but this act has shown he believes access controls shouldn't apply to him.

--
Jeremy Weber [redacted]
DDI/CCI/EDG/AED/OSB
[redacted]

```
==========================================================
Classification: UNCLASSIFIED//~~/AIUO~~

==========================================================
Classification: UNCLASSIFIED//~~/AIUO~~


==========================================================
Classification: ~~SECRET~~

==========================================================
Classification: ~~SECRET~~

==========================================================
Classification: ~~SECRET~~

==========================================================
Classification: ~~SECRET//[redacted]/NOFORN~~
```

==

Classification: ~~SECRET//~~[redacted]~~/NOFORN~~

Classification: ~~SECRET~~

[redacted]

==

Josh,

I discussed things with Sean and this is the situation.

•€€€€€€€€ In the short term, the OSB libraries remain an OSB project and are under Frank Stedman and my guidance.
•€€€€€€€€ You are free to contribute to the libraries by creating a branch and following the pull request model that is in place.
•€€€€€€€€ We are hoping to move the libraries to Kevin’s authority to make them officially an AED level resource.
•€€€€€€€€ When Kevin takes over and if he desires for you to have direct authority for the two long lived branches, then we will give you commit access to master and develop.

Until something officially changes, you must follow the pull request model and leave it to either Frank Stedman or me to complete the merge.

--
Jeremy Weber
DDI/CCI/EDG/AED/OSB
[redacted]

==

Classification: ~~SECRET~~