ellucian®

Banner Enterprise Identity Services and Banner Web Tailor Product Update

Frequently Asked Questions (FAQ)

Updated August 6, 2019 (Version 2.0)

AUGUST 6, 2019 – The U.S. Department of Education (Department) has released an update to its July 17 report that cited a known security vulnerability in the Banner Web Tailor and Banner Enterprise Identity Services (BEIS) offerings.

To date, the Department has not found any instances where the Ellucian Banner vulnerability has been exploited or where it is related to the issues described in the original alert. Additionally, Ellucian has conducted its own research and monitoring that has produced no evidence of any attempt to attack the Banner vulnerability. The Department's research into the impact may be ongoing, and institutions may receive inquiries directly from the Federal Student Aid Cyber Incident Team.

Customer communication:

The following was sent to Banner General customers to the roles of Primary Account Contacts, Key Technical Contacts and Key Security Contacts on July 18, 2019. It was also posted on Banner General and Banner Technical Space on Ellucian Community.

On July 17, 2019, the US Department of Education ("DoE") posted a report that cited a security vulnerability in the Banner Web Tailor offering that could affect a small subset of Banner customers.

Ellucian has confirmed internally there are actually two issues outlined in the Department of Education report. They are separate and unrelated issues and Ellucian has communicated this to the Department of Education:

1. Banner Web Tailor Vulnerability: Ellucian issued patches for the vulnerability in Banner Web Tailor and Banner Enterprise Identity Services on May 14, 2019 and all subsequent roll-up software releases include this fix.

   Only Ellucian customers with Banner Web Tailor versions 8.8.3 and 8.8.4 and Banner Enterprise Identity Services versions 8.3, 8.3.1, 8.3.2, and 8.4 or earlier, should apply the patches. Although it was noted in the Department of Education report as at risk, Banner Web Tailor 8.9 is a roll-up software release that contains all patches and releases since 8.8 and is not affected. Customers who are not on these solutions or who have applied the patches are not affected.

2. Creation of Fraudulent Admissions Applications: This is an industry issue and not specific to Ellucian or Banner. We have published information on how to reduce the impact of these issues on **Ellucian Community**.

If you have questions we are standing by to help. Please contact Ellucian's Customer Center and visit the **Banner General and Banner Technical Space on Ellucian Community** for further updates.

Frequently Asked Questions

Q: How can I confirm that the patch is applied?

A: The Display Banner Versions and Patches (GUIVERS) page is used to display Banner versions and patches by product and the 8.x installed version for each product with the most current version. This page allows you to easily check your installed product versions and patches. You can access this page directly, but it is not found on a menu. It is also accessible through the About Banner (GUAABOT) page or the Installation Controls (GUAINST) page. On either page, click the Display Installed Patch Information button to display the GUIVERS page. You should have two patches installed - one for Banner Enterprise Identity Services (BEIS) and one for Banner Web Tailor. There are four different versions of the patches depending on which version of BEIS they are on:

- For BEIS 8.3, apply patch pcr-000165951_beis8030001 and Web Tailor 8.8.4.1 or 8.9
- For BEIS 8.3.1, apply patch pcr-000165949_beis8030103 and Web Tailor 8.8.4.1 or 8.9
- For BEIS 8.3.2, apply patch pcr-000165948_beis8030203 and Web Tailor 8.8.4.1 or 8.9
- For BEIS 8.4, apply patch pcr-000165947_beis8040004 and Web Tailor 8.8.4.1 or 8.9

Q: BEIS has released another patch since May (pcr-000167489_beis8040005.zip). There have been other releases since May 14, 2019. Which release should I be applying?

A: The June 27th patch of BEIS addressed a specific issue. (CR: 000167489 Malformed (double quote) IDMSESSID cookie is causing session timeouts with the latest BEIS SSO Manager patches for Ellucian Security Alert 20190513). This particular patch was not a specific roll-up software release. We recommend you apply versions:

- For BEIS 8.3, apply patch pcr-000165951_beis8030001 and Web Tailor 8.8.4.1 or 8.9
- For BEIS 8.3.1, apply patch pcr-000165949_beis8030103 and Web Tailor 8.8.4.1 or 8.9
- For BEIS 8.3.2, apply patch pcr-000165948_beis8030203 and Web Tailor 8.8.4.1 or 8.9
- For BEIS 8.4, apply patch pcr-000165947_beis8040004 and Web Tailor 8.8.4.1 or 8.9

Q: If I am not running Banner Enterprise Identity Services (BEIS), do I still need to apply the Banner Web Tailor patch?

A: If you are running **Banner Self-Service, you are likely using SSO Manager** which is a subset of BEIS. Given this, you are impacted. Ellucian recommends applying the patches above.

Q: If your Banner instance leverages a different SSO such as SecureAuth, CAS, etc. (and bypasses the users over SSO Manager), do I still need the two patches?

A: Provided you are not using any components of SSO Manager, you only need to apply the Banner Web Tailor patch with the recommendations above. Regardless of your situation, Ellucian recommends you stay current with all security patches for installed components.

Q: Is Banner Self-Service impacted when localized for supported regions (such as Arabic, Spanish, Portuguese translation packs, etc.)?

A: These issues are related to Banner Enterprise Identity Services and Banner Web Tailor which are leveraged in Banner Self-Service deployments regardless of region. You are potentially impacted by this issue. Ellucian strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update fixes without delay.

Q: Are these two designated patches Multi-Entity Processing (MEP) compatible?

A: Yes, these patches are compatible with MEP deployments.

Q: Do you anticipate this patch release will take a significant amount of time to install and require major regression testing?

A: This is a standard point release patch which is relatively low complexity. There may be some additional interdependencies depending on your environment which are detailed in the Release Notes. If you have any issues with your patch upgrade, please contact Ellucian Customer Support for assistance.

Q: How can we determine if someone attempted to exploit this vulnerability in our environment?

A: If you are not on the latest patches, you should review Banner 8.x Self Service access logs for unusual activity. You would notice error requests coming from the same IP address, likely at high volume. If you have questions about your findings and need insight, please contact Ellucian Customer Support for assistance.

Q: Is the same BEIS and Banner Web Tailor vulnerability applicable to any other Ellucian solutions?

A: No, this issue is specific to Ellucian Banner.

Q: Is the same BEIS and Banner Web Tailor vulnerability related to the Fraudulent Admissions Application issue?

A: No. The creation of Fraudulent Admissions Applications is an industry issue and not specific to Ellucian or any company. We have published information on how to reduce the impact of these issues on Addressing Fraudulent Admissions Applications on **Ellucian Community**.

Q: How hard is it to exploit the vulnerability patched on May 14th, 2019 within Banner Web Tailor and Banner Enterprise Identity Services (BEIS)?

A: This vulnerability is difficult to exploit. In order to exploit this vulnerability, a potential attacker would need to know the UDC ID of the person/account they are attempting to access. That information could be obtained if an attacker knows the Enterprise ID assertion for the user mapped to a Banner person identifier. They would then need details of the session/cookie creation process in order to create a script to facilitate the attack. From that point, the attacker would need to continuously attempt to invoke a logon. The attacker would need to continue to do this until the targeted user logged on, at which point a race condition would occur, with the faster connection being granted the logon.

Q: What communications were delivered on the original security patches for Banner Web Tailor and BEIS?

A: On May 14, 2019, the original Banner Web Tailor and BEIS security patches were delivered via the Ellucian Customer Center and posted in the Ellucian Community here within the Banner General and Banner Technical space.

Q: Does this vulnerability apply to Banner 8.x or 9.x Administrative applications?

A: No. These do not affect Banner 8.x Administrative or Banner 9.x Administrative applications. These issues are related to Banner Enterprise Identity Services and Banner Web Tailor which are leveraged in Banner Self-Service deployments.

Q: One article states that student data was stolen, does Ellucian have information to support this claim?

A: No, we have no reported incidents where this vulnerability has been successfully exploited.