مرکز تخصصی

آپا

دانشگاه صنعتی اصفهان

(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

ارزیابی امنیتی سامانه معاونین توسعه دانشگاه‌های علوم پزشکی کشور

مربوط به :

شرکت فرادید رایان افزار

(محرمانه)

آبان‌ماه ۱۳۹۸

مقدمه

این گزارش بنا به درخواست شرکت مهندسی " فرادید رایان افزار" توسط مرکز تخصصی آپا دانشگاه صنعتی اصفهان تهیه شده است. نتایج ارزیابی نشان‌دهنده وجود آسیب‌پذیری با سطح خطر بالا می‌باشد.

هدف اصلی این گزارش، اعلام مجموعه آسیب‌پذیری‌های شناسایی شده در سامانه مورد نظر جهت رفع و ارتقاء امنیت می‌باشد. در گزارش ارزیابی امنیتی علاوه بر آسیب‌پذیری برنامه کاربردی تحت وب، به تعدادی از آسیب‌پذیری‌های ماشین سرویس‌دهنده نیز اشاره شده است. آسیب‌پذیری‌های ماشین سرویس‌دهنده صرفاً جنبه آگاهی‌رسانی داشته و در صدور گواهی موثر نیستند.

این ارزیابی با شرایط ذیل انجام شده است:

سامانه تحت ارزیابی	سامانه معاونین توسعه دانشگاه های علوم پزشکی کشور
نوع کارگزار وب	IIS/10
فناوری توسعه	DNN v. 09.04.01 (22)
پایگاه داده	Microsoft SQL Server 2017
سیستم‌عامل	Microsoft Windows Server 2016 Standard
نوع ارزیابی	آزمون نفوذپذیری جعبه‌سیاه با سطح دسترسی کاربر
زمان ارزیابی	
شرایط ارزیابی	ارزیابی در محل فیزیکی سرویس‌دهنده انجام شده است.

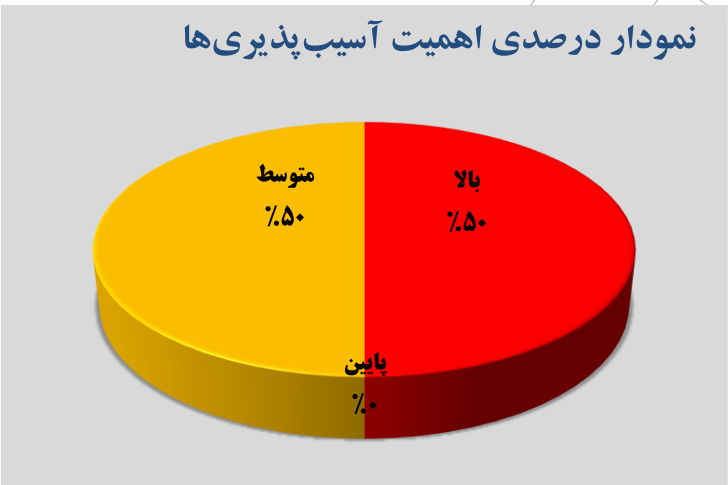
ارزیابی سرویس‌دهنده و برنامه‌های کاربردی

- ارزیابی‌ها نشان می‌دهد که پورت‌های زیر بر روی ماشین سرویس‌دهنده باز می‌باشند (صرفاً جهت آگاهی):

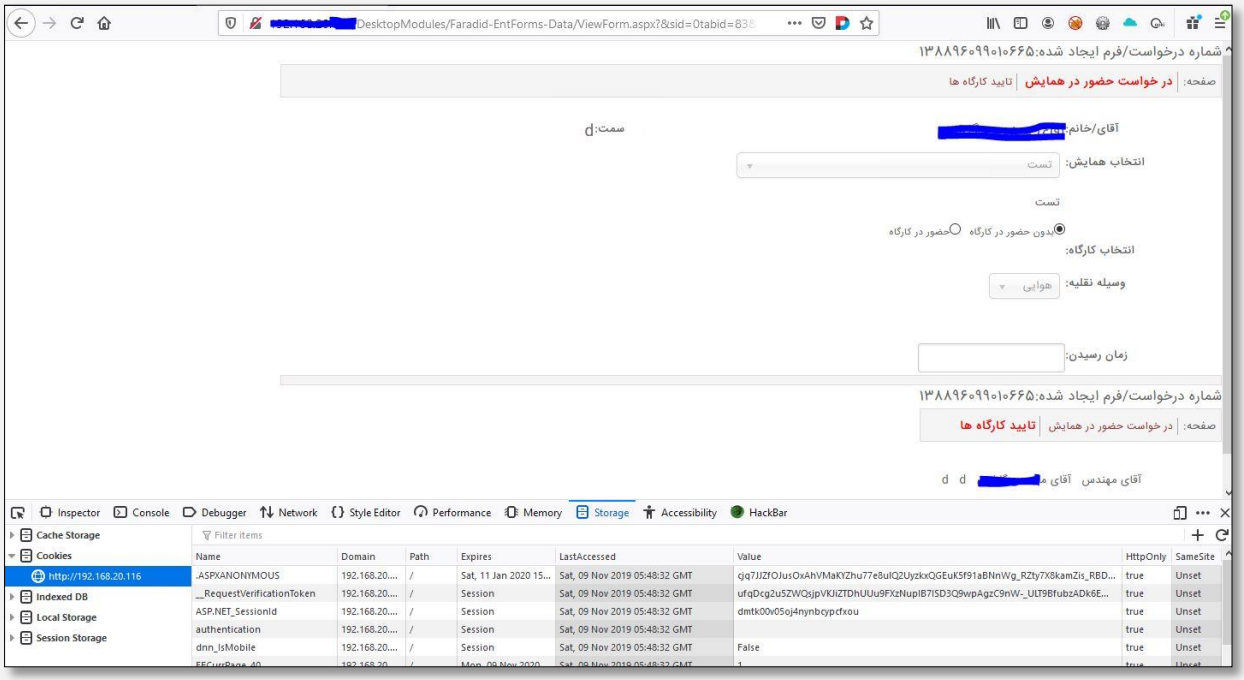
ردیف	شماره پورت	سرویس
۱	80/tcp	http
۲	135/tcp	msrpc
۳	139/tcp	smb
۴	445/tcp	cifs

➢ وضعیت آسیب‌پذیری‌های کشف شده عبارتند از:

درجه آسیب پذیری	تعداد
بالا	۲
متوسط	۲
پایین	۰



بررسی‌های انجام گرفته نشان می‌دهد که در برنامه کاربردی تحت‌وب **"سامانه معاونین توسعه دانشگاه های علوم پزشکی کشور"** ، آسیب‌پذیری‌های زیر وجود دارند:

نام آسیب‌پذیری: کنترل دسترسی نامناسب
آدرس‌های آسیب‌پذیر: • /DesktopModules/Faradid-EntForms/ViewForm.aspx?&sid=….
سطح خطر: بالا
توضیح مختصر: عدم کنترل دسترسی مناسب به صفحات مختلف وب سایت می‌تواند منجر به افشای اطلاعات محرمانه یک سیستم شود. باید تمامی داده‌ها و صفحات هنگام بارگذاری بررسی شوند که آیا کاربر جاری مجاز به مشاهده این اطلاعات می‌باشد؟ عدم کنترل دسترسی مناسب می‌تواند سیستم را با چالش‌های حفظ حریم خصوصی نیز روبه‌رو کند.
راه‌حل : بررسی دسترسی‌ها در هنگام پاسخ به درخواست‌ها.
اثبات: در این سامانه صفحه مربوط به چاپ اطلاعات کارت ورود دچار ضعف امنیتی است. با دستکاری پارامترهای موجود در لینک صفحه می‌توان به اطلاعات کارت ورود دیگر کاربران دست یافت. 

نام آسیب‌پذیری: ارسال نام کاربری و رمز عبور به‌صورت فاش
آدرس آسیب‌پذیر: • /
سطح خطر: بالا
توضیح مختصر: فرم login به صورت رمز نشده از سمت کاربر به سوی سرور فرستاده می شود. درنتیجه رمز کاربران به‌صورت فاش از بستر اینترنت عبور می‌کند و در صورت شنود شبکه رمز کاربران فاش خواهد شد.
راه‌حل: استفاده از https به‌جای http

نام آسیب‌پذیری : بارگذاری فایل کنترل نشده
آدرس آسیب‌پذیر : • /API/InternalServices/FileUpload/UploadFromLocal
سطح خطر: متوسط
توضیح مختصر: بارگذاری فایل روی کارگزار سامانه می‌تواند باعث شود سامانه با مخاطراتی رو به رو شود. زیرا ممکن است فایل‌های آلوده به بدافزار روی سامانه قرار گیرند. برای کاهش این مخاطرات باید کنترل‌هایی در سمت کلاینت و کارگزار انجام شود. یکی از این کنترل‌ها بررسی نوع فایل می‌باشد.
راه‌حل : علاوه بر پسوند فایل‌ها باید سرآیند فایل نیز بررسی شود.

نام آسیب‌پذیری: خطای کنترل نشده

آدرس‌های آسیب‌پذیر:

- /
- /WebResource.axd
- /ScriptResource.axd
- /desktopmodules/DNNArticleLightboxContentPlugin/Thumbnail.ashx
- /Default.aspx
- /Home/AppointmentRequest/

سطح خطر: متوسط

تو ضیح مخت صر: طبق ارزیابی انجام شـده مشـخص گردید، صـفحات زیر حاوی پیغام‌های error/warning می‌با شند. این صفحات ممکن ا ست اطلاعات حـ سا سی را فاش نمایند. به‌علاوه این اطلاعات ممکن ا ست محل ذخیره‌ی فایلی که باعث ایجاد استثناء مدیریت نشده است را نیز نشان دهد. این اطلاعات فاش شده می‌تواند به مهاجم برای اجرای موفق حملات بعدی کمک نماید.

راه‌حل : پیشـنهاد می‌گردد کد منبع صـفحه مربوطه مورد بازبینی قرار گیرد. همچنین صـفحه خطا دلخواه برای نمایش به کاربر پیاده‌سـازی گردد. اسـتفاده از روش واحد برای handling خطاها که حاوی هیچ‌گونه اطلاعاتی همچون مکان قرارگیری فایلی که خطا در آن رخ داده است نباشد.

اثبات آسیب پذیری: