بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

گزارش اصلاحیه امنیتی مایکروسافت در می ۲۰۱۸

اردیبهشت ۹۷

مقدمه

مرکز پاسخگویی امنیتی مایکروسافت (MSRC) بصورت دوره‌ای گزارش‌های مربوط به آسیب‌پذیری‌های امنیتی محصولات و خدمات مایکروسافت را بررسی می‌کند و اطلاعات تجمیعی را با هدف کمک به مدیریت تهدیدات امنیتی و حفاظت از سیستم‌های استفاده کنندگان فراهم می‌نماید. بسته بروزرسانی امنیتی ماه می مایکروسافت شامل بروزرسانی‌های امنیتی برای نرم افزارهای زیر است:

۱. Internet Explorer
۲. Microsoft Edge
۳. Microsoft Windows
۴. Microsoft Office and Microsoft Office Services and Web Apps
۵. ChakraCore

در این گزارش فهرست آسیب پذیری‌های منتشر شده در بازه زمانی 04/11/2018 الی 05/10/2018 با درجه حساسیت critical و important مورد بررسی قرار گرفته است.

نام محصول	Office
نام آسیب پذیری	Microsoft Office Remote Code Execution Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2018-8157 CVE-2018-8158 CVE-2018-8161
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	05/08/2018
توضیحات	آسیب پذیری موجود به دلیل دسترسی نادرست نرم افزار Microsoft Office به اشیاء در حافظه به وجود می آید. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند. • می تواند به مشاهده، تغییر یا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8161 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8157 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8158

نام محصول	Office
نام آسیب پذیری	Microsoft Excel Remote Code Execution Vulnerability
حساسیت	Critical

شناسه آسیب‌پذیری	CVE-2018-8147 CVE-2018-8148 CVE-2018-8162
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	05/08/2018
توضیحات	آسیب پذیری موجود به دلیل دسترسی نادرست نرم افزار Microsoft Excel به اشیاء در حافظه به وجود می آید. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8147 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8148 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8162

نام محصول	**Chakra Core**
نام آسیب پذیری	**Scripting Engine Memory Corruption Vulnerability**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2018-0954 CVE-2018-0946 CVE-2018-0943 CVE-2018-0945 CVE-2018-0953 CVE-2018-1022 CVE-2018-8128 CVE-2018-8130

	CVE-2018-8133 CVE-2018-8137 CVE-2018-8139 CVE-2018-8177 CVE-2018-8178 CVE-2018-8115
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	05/08/2018
توضیحات	آسیب پذیری موجود در Chakra Core به دلیل نحوه ی نادرست قراردادن اشیاء در حافظه توسط موتور اسکریپت چاکرا ایجاد می شود. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ... به دلیل اینکه سورس کد موتور چاکرا در گیتاپ مایکروسافت وجود دارد هکرها با بررسی سورس کد برنامه موفق به کشف آسیب پذیری در آن شدند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0943 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0945 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0946 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0953 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0954 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1022 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8128 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8130 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8133 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8137

	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8139 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8177 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8178 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8115

نام محصول	Microsoft Exchange Server۲۰۱۰-۲۰۱۳-۲۰۱۶
نام آسیب‌پذیری	Microsoft Exchange Memory Corruption Vulnerability
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2018-8154
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	05/08/2018
توضیحات	آسیب پذیری موجود به دلیل دسترسی نادرست نرم افزارMicrosoft Exchangeبه اشیاء در حافظه به وجود می آید. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8154

نام محصول	Microsoft Edge
نام آسیب پذیری	Scripting Engine Memory Corruption Vulnerability

حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2018-0943 CVE-2018-0945 CVE-2018-0946 CVE-2018-0951 CVE-2018-0953 CVE-2018-0954 CVE-2018-0955 CVE-2018-1022 CVE-2018-8128 CVE-2018-8130 CVE-2018-8133 CVE-2018-8137 CVE-2018-8139 CVE-2018-8178 CVE-2018-8179
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	05/08/2018
توضیحات	آسیب پذیری موجود در Microsoft Edge که به دلیل نحوه ی نادرست قراردادن اشیاء در حافظه توسط موتور اسکریپت چاکرا ایجاد می شود. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...

	به دلیل اینکه سورس کد موتور چاکرا در گیتاپ مایکروسافت وجود دارد هکرها با بررسی سورس کد برنامه موفق به کشف آسیب پذیری در آن شدند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0943 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0945 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0946 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0951 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0953 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0954 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0955 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1022 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8128 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8130 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8133 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8137 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8139 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8178 /CVE-2018-8179https://portal.msrc.microsoft.com/en-US/security-guidance/advisory

نام محصول	**Internet Explorer 11**
حساسیت	Critical
شناسه آسیب‌پذیری	CVE-2018-8114 CVE-2018-8122
تاثیر	Remote Code Execution
آخرین به‌روزرسانی	05/08/2018
توضیحات	آسیب پذیری موجود به دلیل دسترسی نادرست Internet Explorer به اشیاء در حافظه به وجود می آید. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه

	را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8114 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8122

نام محصول	**Windows**
نام آسیب پذیری	**Win32k Elevation of Privilege Vulnerability**
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-8120 CVE-2018-8124 CVE-2018-8164 CVE-2018-8165
تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	با استفاده از این آسیب پذیری مهاجم می تواند سطح دسترسی خود را در سیستم عامل ارتقا دهد. این آسیب پذیری به دلیل مدیریت نامناسب اشیاء در حافظه توسط componentهای Win32k به وجود می آید. این آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد.

	• حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8120 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8124 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8164 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8165

نام محصول	**Windows**
نام آسیب پذیری	**Windows Kernel Elevation of Privilege Vulnerability**
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-8897
تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	با استفاده از این آسیب پذیری مهاجم می تواند سطح دسترسی خود را در سیستم عامل ارتقا دهد. این آسیب پذیری به دلیل مدیریت نامناسب اشیاء در حافظه توسط هسته سیستم به وجود می آید. این آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8897

نام محصول	Windows
نام آسیب پذیری	Windows Elevation of Privilege Vulnerability
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-8134
تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	با استفاده از این آسیب پذیری مهاجم می تواند سطح دسترسی خود را در سیستم عامل ارتقا دهد. این آسیب پذیری در مجوزهای اجرای توابع API مربوط به کرنل وجود دارد. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8134

نام محصول	Windows
نام آسیب پذیری	Windows Image Elevation of Privilege Vulnerability
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-8170

تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	با استفاده از این آسیب پذیری مهاجم می تواند سطح دسترسی خود را در سیستم عامل ارتقا دهد. این آسیب پذیری به دلیل دسترسی نادرست kernel image به اشیاء در حافظه به وجود می آید. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8170

نام محصول	**Windows**
نام آسیب پذیری	**Windows Common Log File System Driver Elevation of Privilege Vulnerability**
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-8167
تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	با استفاده از این آسیب پذیری مهاجم می تواند سطح دسترسی خود را در سیستم عامل ارتقا دهد. این آسیب پذیری به دلیل دسترسی نادرست Windows Common Log File System (CLFS)به اشیاء در حافظه به وجود می آید. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم

	بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8167

نام محصول	**Windows**
نام آسیب پذیری	**Windows Common Log File System Driver Elevation of Privilege Vulnerability**
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-8165
تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	با استفاده از این آسیب پذیری مهاجم می تواند سطح دسترسی خود را در سیستم عامل ارتقا دهد. این آسیب پذیری به دلیل دسترسی نادرست درایور DirectX Graphics Kernel (DXGKRNL) به اشیاء در حافظه به وجود می آید. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد.

	•یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8167

نام محصول	**Share Point**
نام آسیب پذیری	**Microsoft SharePoint Elevation of Privilege Vulnerability**
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-8149 CVE-2018-8155 CVE-2018-8168 CVE-2018-8156
تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	این آسیب پذیری زمانی رخ می دهد که Microsoft SharePoint Server به طور مناسب درخواست وب را به یک سرور مربوط به شیرپوینت پاسخ نمی‌دهد. یک مهاجم می تواند با ارسال یک درخواست خاص به یک سرور تاثیر شیرپوینت، از آسیب پذیری بهره برداری کند. مهاجم می‌تواند حملات اسکریپت cross-site را به سیستم های آسیب دیده انجام دهد و اسکریپت را در محیط کاربر فعلی اجرا کند. این حملات می تواند مهاجم را مجاز به خواندن محتوایی که مجاز به خواندن آن نیست، نماید و همچنین از هویت قربانی برای انجام اقدامات در سایت شیرپوینت ، مانند تغییر و حذف محتوا استفاده کند و یا محتوای مخرب را در مرورگر کاربر تزریق کند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8167

نام محصول	Microsoft infopath
نام آسیب پذیری	Microsoft InfoPath Remote Code Execution Vulnerability
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-8173
تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	با استفاده از این آسیب پذیری مهاجم می تواند سطح دسترسی خود را در سیستم عامل ارتقا دهد. این آسیب پذیری به دلیل عدم دسترسی Microsoft Infopath به اشیاء در حافظه به وجود می آید. آسیب پذیری می تواند حافظه را به گونه ای تخریب کند که یک مهاجم بتواند کد دلخواه را در چارچوب کاربر فعلی با همان سطح دسترسی اجرا کند. در نتیجه اگر کاربر با حساب کاربری مدیر وارد شود مهاجم توانایی فعالیت های زیر را خواهد داشت: • برنامه ها را نصب و یا حذف کند • می تواند به مشاهده، تغییریا حذف داده ها بپردازد. • حساب کاربری جدید با دسترسی کامل برای خود بسازد. •یک در پشتی ایجاد کند. و ...
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8173

نام محصول	Microsoft Exchange Server
نام آسیب پذیری	Microsoft Exchange Server Elevation of Privilege Vulnerability
حساسیت	Important

شناسه آسیب‌پذیری	CVE-2018-8152
تاثیر	Elevation of Privilege
آخرین به‌روزرسانی	05/08/2018
توضیحات	این آسیب پذیری به دلیل مدیریت نامناسب اشیاء در حافظه توسط Microsoft Exchange Outlook Web Access (OWA) رخ می دهد. این حمله با ارسال ایمیل مخرب به سوی کاربر انجام می پذیرد. در صورتی که مهاجم به درستی از این آسیب پذیری بهره برداری کند می تواند اسکریپت های مورد نیاز خود را بر روی سیستم قربانی اجرا کند و اطلاعات حساسی را از او بدست آورد. مهاجم برای سواستفاده از این آسیب‌پذیری لازم است یک لینک را برای قربانی فرستاده تا به روش مهندسی اجتماعی بتواند کاربر را مجاب به باز کردن لینک کند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8152

نام محصول	**.NET**
نام آسیب پذیری	**.NET and .NET Core Denial of Service Vulnerability**
حساسیت	Important
شناسه آسیب‌پذیری	CVE-2018-0765
تاثیر	Denial of Service
آخرین به‌روزرسانی	05/08/2018

توضیحات	این آسیب پذیری از نوع منع سرویس (DOS) و بر روی نرم افزار .net و .net core می باشد. این آسیب پذیری در پردازش فایل XML رخ می دهد. مهاجم می تواند با ارسال درخواست مخرب خاص به سمت برنامه .net این حمله را ایجاد کند.
رفع آسیب‌پذیری	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0765