مرکزماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش اصلاحات امنیتی محصولات سیسکو با درجه حساسیت Critical در August ۲۰۱۹

بحرانی(Critical)	Cisco Small Business 220 Series Smart Switches Remote Code Execution Vulnerabilities
عنوان	آسیب پذیری اجرای کد از را دور سوئیچ های هوشمند سری **Small Business 220** سیسکو
شناسه آسیب‌پذیری	**CVE-2019-1913**
CVSS Score	Base – 9.8
نسخه	1.0 final
شناسه باگ‌های سیسکو	CSCvo78320
تاثیر	Remote Code Execution Vulnerabilities
تاریخ آخرین به‌روزرسانی	2019 August 6 14:00 GMT
توضیحات	آسیب پذیری چندگانه موجود در رابط مدیریت web سوئیچ‌های هوشمند Cisco Small Business 220 Series می‌تواند باعث دسترسی یک مهاجم تصدیق نشده به سیستم شود. این حملات با سرریز بافر و دسترسی به عنوان کاربر root و اجرایی کد دلخواه پایان می‌یابد.
محصولات آسیب‌پذیر	این آسیب‌پذیری بر روی سوئیچ های هوشمند سری Cisco Small Business 220 که رابط web مدیریتی را در نسخه هایی قبل ۱.۱.۴.۴ فعال می‌کنند، وجود دارد. توجه شود که رابط مدیریت web به صورت پیش فرض از طریق HTTP یا HTTPS فعال می‌شود.
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-auth_bypass

بحرانی(Critical)	Cisco Small Business 220 Series Smart Switches Authentication Bypass Vulnerability
عنوان	آسیب‌پذیری دور زدن احراز هویت سوئیچ های هوشمند سری Small Business 220 سیسکو
شناسه آسیب‌پذیری	CVE-2019-1912
CVSS Score	Base – 9.1
نسخه	1.0 final
شناسه باگ‌های سیسکو	CSCvo78300
تاثیر	Authentication Bypass Vulnerability
تاریخ آخرین به‌روزرسانی	2019 August 6 14:00 GMT
توضیحات	آسیب پذیری موجود در رابط مدیریت web سوئیچ های هوشمند Cisco Small Business 220 Series می‌تواند باعث دسترسی مهاجم تصدیق نشده از راه دور شود که می تواند فایل مورد نظر خود را بر روی سیستم بارگذاری نماید.
محصولات آسیب‌پذیر	این آسیب‌پذیری بر روی سوئیچ های هوشمند سری Cisco Small Business 220 که رابط web مدیریتی را در نسخه هایی قبل ۱.۱.۴.۴ فعال می‌کنند، وجود دارد. توجه شود که رابط مدیریت web به صورت پیش فرض از طریق HTTP یا HTTPS فعال می‌شود.
راه حل	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-rce