بسمه تعالی

مرکز ماهر
مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

حملات Address bar spoofing به مرورگرهای موبایلی

هشدار

شناسه سند ..... MaherReport_13990801-01

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۳۹۹/۰۷/۳۰

طبقه‌بندی سند ..... **عادی**

تهران، خیابان بهشتی، نرسیده به قائم مقام، معاونت امنیت فضای تولید و تبادل اطلاعات، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰

(۰۲۱) ۴۲۶۵۰۰۰۰

cert.ir

فهرست مطالب

۱ حملات Address bar spoofing به مرورگرهای موبایلی

منظور از آسیب‌پذیری Address bar spoofing ضعفی در مرورگر است که به وب‌سایت آلوده این امکان را می‌دهد تا URL جایگزینی را بجای URL واقعی وب‌سایت به کاربر نمایش دهد.

در مرورگرهای دسکتاپی چندین قابلیت و ویژگی برای شناسایی تغییرات در URL موجود است؛ اما این امکانات امنیتی در مرورگرهای موبایلی به دلیل اندازه کوچک صفحه‌نمایش و عدم وجود برخی از ویژگی‌های امنیتی، موجود نیست.

ده مورد از این آسیب‌پذیری در ۷ مرورگر موبایلی نام‌آشنا، از قبیل Apple Safari، Opera Touch و Opera Mini و مرورگرهای دیگری همچون Bolt، RITS، UC Browser و Yandex Browser دیده می‌شود. در اوایل سال جاری میلادی این موارد شناسایی و در ماه اگوست به سازندگان مرورگرها اعلان شد. سازندگان نام‌آشنا به‌صورت آنی وصله‌های لازم را ارائه دادند ولی سازندگان دیگر هیچ اقدامی در این خصوص انجام ندادند. در جدول ۱ لیست آسیب‌پذیری آورده شده است.

جدول ۱- لیست آسیب‌پذیری

شناسه آسیب‌پذیری	شرکت سازنده	مرورگر	نسخه	پلتفرم	آیا اصلاحیه‌ای انجام‌شده؟
CVE-2020-7363	UCWeb	UC Broser	13.0.8	اندروید	پاسخی از طرف شرکت سازنده دریافت نشده است.
CVE-2020-7364	UCWeb	UC Broser	13.0.8	اندروید	پاسخی از طرف شرکت سازنده دریافت نشده است.
CVE TBD-Opera	Opera	Opera Mini	51.0.2254	اندروید	در ۱۱ نوامبر سال ۲۰۲۰ رفع خواهد شد.
CVE TBD-Opera	Opera	Opera Touch	2.4.4	iOS	در ۱۱ نوامبر سال ۲۰۲۰ رفع خواهد شد.
CVE TBD-Opera	Opera	Opera Touch	2.4.4	iOS	در ۱۱ نوامبر سال ۲۰۲۰ رفع خواهد شد.
CVE TBD-Opera	Opera	Opera Touch	2.4.4	iOS	در ۱۱ نوامبر سال ۲۰۲۰ رفع خواهد شد.

CVE-2020-7369	Yandex	Yandex Browser	20.8	اندروید	پاسخ داده شده اما پیگیری صورت نگرفته است.
CVE-2020-7370	Danyil Vasilenko	Bolt Browser	1.4	iOS	ایمیل پشتیبانی ریجکت شده و امنیت اپل را تغییر داده است
CVE-2020-7371	Raise IT Solutions	RITS Browser	3.3.9	اندروید	پاسخی از طرف شرکت سازنده دریافت نشده است.
CVE-2020-7387	Apple	Safaro	iOS 13.6	iOS	اصلاحیه منتشر شده است.

بنا به مطالعات انجام‌شده می‌توان نتیجه گرفت که این آسیب‌پذیری با ایجاد تداخل مابین زمان بارگذاری صفحه و زمان رفرش (Refresh) آدرس URL، منجر به نمایش آدرس اشتباه به کاربر می‌گردد. بنابراین بهره‌برداری از این باگ، مستلزم استفاده کاربر از مرورگر منسوخ‌شده و بازدید کاربر از سایت آلوده است.

با توجه به موارد گفته‌شده می‌توان نتیجه گرفت که اجرای این حملات بسیار ساده و راحت است. پس پیشنهاد می‌شود که کاربران هرچه سریع‌تر مرورگر خود را به‌روزرسانی کرده یا از مرورگرهای فاقد این آسیب‌پذیری استفاده نمایند.

منبع:

https://www.zdnet.com/article/seven-mobile-browsers-vulnerable-to-address-bar-spoofing-attacks/#ftag=RSSbaffb68