بسمه تعالی

مرکز ماهر

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

آسیب‌پذیری بحرانی در محصول BIG-IP

گزارش آسیب‌پذیری محصول

شناسه سند ..... Maher Report_13990415-3

نوع سند ..... گزارش فنی

شماره نگارش ۱/۰

تاریخ نگارش ۱۳۹۹/۰۴/۱۵

طبقه‌بندی سند ..... **عادی**

تهران- میدان آرژانتین- ابتدای بلوار بیهقی- نبش خیابان شانزدهم- ساختمان شماره ۱ سازمان فناوری اطلاعات ایران

(۰۲۱)۴۲۶۵۰۰۰۰

۴۲۶۵۰۰۰۰ ۰۲۱

cert.ir

فهرست مطالب

۱ مقدمه

اجرای کد از راه دور در دستگاه‌های F5 BIG-IP، دولت‌ها، ارائه دهندگان فضای ابری، ISPها، بانک‌ها و بسیاری از شرکت‌های Fortune 500 را در معرض حملات احتمالی قرار می‌دهد. F5 Networks یکی از بزرگترین شرکت‌های ارائه‌دهنده تجهیزات شبکه در سراسر جهان، این هفته یک مشاوره امنیتی را منتشر کرده است که به مشتریان خود توصیه می‌کند که یک نقص امنیتی خطرناک را که به احتمال زیاد مورد اکسپلویت قرار گرفته است، وصله نمایند.

این آسیب‌پذیری، محصول BIG-IP این شرکت را تحت تاثیر قرار می‌دهد. BIG-IP دستگاه‌های چندمنظوره شبکه هستند که می‌توانند به عنوان سیستم‌های شکل‌دهی ترافیک وب، لود بالانسرها، فایروال‌ها، دروازه‌های دسترسی (access gateways)، rate limiterها یا SSL middleware کار کنند. BIP-IP یکی از محبوبترین محصولات شبکه است که به صورت روزانه در شبکه‌های دولتی در سراسر جهان، در شبکه‌های مربوط به ارائه‌دهندگان خدمات اینترنت، در مراکز داده محاسبات ابری و به طور گسترده در شبکه‌های سازمانی مورد استفاده قرار می‌گیرد.

آسیب‌پذیری بحرانی مذکور با شناسه CVE-2020-5902 و شدت ۱۰ به‌طور دقیق‌تر در ماژول TMUI (Traffic Management User Interface) وجود دارد و توسط یک محقق امنیتی به شرکت F5 گزارش شده است. مهاجم می‌تواند با ارسال یک درخواست مخرب HTTP به سروری که از ماژول TMUI استفاده می‌کند، از آسیب‌پذیری بهره‌برداری کند. بهره‌برداری از این آسیب‌پذیری امکان اجرای کد از راه دور و شنود ترافیک شبکه را فراهم می‌کند. پس از بهره‌برداری مهاجم قادر است:

- فایل‌های موجود را حذف و یا فایل جدیدی ایجاد کند
- سرویس‌ها را غیرفعال کند
- اطلاعات را شنود کند
- دستورات (کامند) دلخواه سیستمی یا کدهای جاوا اجرا کند
- دستگاه BIG-IP را به‌طور کامل در اختیار گیرد
- اهداف دیگری مانند نفوذ به شبکه داخلی را دنبال کند

۲ آسیب‌پذیری CVE-2020-5902

این آسیب‌پذیری (باگ BIG-IP) با شناسه CVE-2020-5902، توسط فردی به نام Mikhail Klyuchnikov، از محققان امنیتی شرکت Positive Technologies، کشف شده و به صورت محرمانه به شرکت F5 گزارش

داده شده است. این باگ که "اجرای کد از راه دور" نیز نامیده می‌شود، در واقع مشکل رابط مدیریت BIG-IP است که به TMUI (Traffic Management User Interface) شهرت دارد.

مهاجمان می‌توانند این باگ را از طریق اینترنت اکسپلویت نموده و به TMUI که روی یک سرور Tomcat و دارای سیستم‌عامل مبتنی بر لینوکس در حال اجرا است دسترسی پیدا کنند. مهاجمان برای حمله به دستگاه‌های آسیب‌پذیر به اطلاعات ورود نیاز ندارند، و یک اکسپلویت موفق می‌تواند برای مهاجمان امکان اجرای دستورات سیستمیِ دلخواه را فراهم نماید. این دستورات می‌توانند حذف فایل‌ها، غیرفعال نمودن سرویس‌ها و اجرای کدهای دلخواه به زبان جاوا باشند. حتی این امکان وجود دارد که مهاجم بتواند کنترل کامل دستگاه BIG-IP را در دست بگیرد.

آسیب‌پذیری مذکور به حدی خطرناک است که در سیستم امتیازدهی CVSSv3 امتیاز ۱۰ از ۱۰ به آن اختصاص یافته است. این بدان معناست که این باگ به سادگی قابل اکسپلویت بوده و از طریق اینترنت می‌تواند مورد سوءاستفاده قرار گیرد، و برای استفاده از آن نیازی به اطلاعات ورود یا مهارت‌های کدنویسی پیشرفته نیست.

به طور کاملاً تصادفی، پس از کشف آسیب‌پذیری بحرانی در دستگاه‌های فایروال و Palo Alto Networks VPN در روز دوشنبه، این دومین آسیب‌پذیری خطرناک با شدت ۱۰ در دستگاه‌های شبکه است که در این هفته افشاء می‌شود.

۳ وصله فوری

فرماندهی سایبری ایالات متحده در هفته جاری هشدارهایی را به بخش‌های خصوصی و دولت صادر کرد تا نقص موجود در Palo Alto را وصله کنند زیرا همان‌طور که انتظار می‌رفت، هکرها اقدام به اکسپلویت این آسیب‌پذیری کرده‌اند.

تاکنون هیچ هشدار رسمی توسط آژانس امنیت سایبری ایالات متحده صادر نشده است؛ اما گفتنی است که نقص F5، به اندازه نقص Palo Alto خطرناک نیست.

Nateبه گفته محققان،به خطر افتادن کامل یک سیستم از نظر تئوری می‌تواند به افراد اجازه دهد تا ترافیک رمزگذاری نشده داخل دستگاه را مورد جاسوسی قرار دهند. سیستم‌عامل مدیریت این دستگاه‌ها، مبتنی بر لینوکس است و مانند اکثر ADCها[۱]، در بخش‌های اصلی و پردسترس شبکه مستقر می‌شوند.

[۱] application delivery controllers

در حال حاضر بر اساس بررسی‌های Shodan ، ۸،۴۰۰ دستگاه BIG-IP به صورت آنلاین متصل هستند. چندین شرکت و محقق امنیتی در حوزه امنیت سایبری به ZDNet خاطر نشان کردند که هیچ حمله‌ای که این دستگاه‌ها را مورد هدف قرار داده باشد، کشف نکرده‌اند؛ اما آن‌ها انتظار دارند که حملات به زودی آغاز شود، بخصوص اگر یک کد اکسپلویت proof-of-concept، به صورت آنلاین منتشر شود.

پیشنهاد می‌شود هر چه سریع‌تر به به‌روزرسانی به نسخه‌ی امن اقدام شود. درصورتی‌که امکان به‌روزرسانی وجود ندارد می‌توان خطرات احتمالی بهره‌برداری از آسیب‌پذیری را در سه بخش کاهش دهید:

در همه‌ی interface های شبکه به httpd المان پیکربندی LocationMatch را اضافه کنید:

- از طریق دستور زیر به TMOS Shell (tmsh) لاگین شود:

```
>tmsh
```

- از طریق دستور زیر httpd ویرایش شود:

```
>edit /sys httpd all-properties
```

- قسمت include به شکل زیر تغییر داده شود:

```
include'
>LocationMatch<"⁎.;.\.\⁎."
Redirect 404/
/>LocationMatch<
'
```

- از طریق دستور زیر فایل تغییرات اعمال و فایل را ذخیره شود:

```
Esc
:wq!
```

- پیکربندی از طریق دستور زیر ذخیره شود:

```
> save /sys config
```

و در آخر از طریق دستور زیر سرویس httpd ، restart شود:

```
> restart sys service httpd
```

- با استفاده از Self IPs دسترسی‌ها به TMUI سیستم BIG-IP بلاک شود. برای این منظور تنظیمات **Port Lockdown** برای هر Slef IP موجود در سیستم به **Allow None** تغییر یابد. اگر نیاز است که پورتی باز شود از Allow Custom برای جلوگیری از دسترسی به TMUI استفاده شود.
- همچنین اجازه‌ی دسترسی «مدیریت» به محصولات F5 باید در بستر یک شبکه **امن** صورت گیرد.

برای اطلاعات بیشتر جهت کاهش خطرات این آسیب‌پذیری به لینک زیر مراجعه کنید:
https://support.f5.com/csp/article/K52145254

۴ محصولات تحت تأثیر این آسیب‌پذیری

جدول ۱ محصولات تحت تأثیر این آسیب

محصولات تحت تأثیر	شاخه	نسخه‌های آسیب‌پذیر	نسخه‌های وصله شده	شدت آسیب‌پذیری	CVSSv۳ امتیاز	مؤلفه و ویژگی آسیب‌پذیری
BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM)	۱۵.x	۱۵.۱.۰	۱۵.۱.۰.۴	بحرانی	۱۰.۰	TMUI/Configuration utility
		۱۵.۰.۰	-			
	۱۴.x	۱۴.۱.۰ - ۱۴.۱.۲	۱۴.۱.۲.۶			
	۱۳.x	۱۳.۱.۰ - ۱۳.۱.۳	۱۳.۱.۳.۴			
	۱۲.x	۱۲.۱.۰ - ۱۲.۱.۵	۱۲.۱.۵.۲			
	۱۱.x	۱۱.۶.۱ - ۱۱.۶.۵	۱۱.۶.۵.۲			
BIG-IQ Centralized Management	۷.x	-	غیرقابل استفاده	آسیب‌پذیر نیست	-	-
	۶.x	-	غیرقابل استفاده			
	۵.x	-	غیرقابل استفاده			
Traffix SDC	۵.x	-	غیرقابل استفاده	آسیب‌پذیر نیست	-	-

۵ منابع

https://www.zdnet.com/article/f5-patches-vulnerability-that-received-a-cvss-10-severity-score/#ftag=RSSbaffb68

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5902

https://support.f5.com/csp/article/K52145254