بسمه تعالی

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

رفع ۵ آسیب‌پذیری بحرانی در روترهای D-Link

خبر آسیب‌پذیری

شناسه سند ..... Maher_13990511-01
نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۰۵/۰۷
طبقه‌بندی سند ..... **عادی**

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

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

1 مقدمه ۱
۲ محصولات تحت تأثیر ۱
۳ جزئیات فنی و روش‌های بهره‌برداری ۱
۴ توصیه امنیتی ۳
۵ منابع ۳

۱ مقدمه

شرکت D-Link به رفع پنج آسیب‌پذیری موثر بر روی روترهای این شرکت با شدت‌های متوسط، بالا و بحرانی پرداخته است. با اکسپلویت این آسیب‌پذیری‌ها توسط مهاجمان، روترهای آسیب‌پذیر و به دنبال آن، شبکه به خطر خواهد افتاد. متأسفانه برخی از روترهای تحت تأثیر این آسیب‌پذیری‌ها، به وضعیت‌های EOS[۱] و یا EOL[۲] رسیده و این شرکت دیگر از آن‌ها پشتیبانی نخواهد کرد و این بدان معناست که بروزرسانی‌های امنیتی را نیز دریافت نخواهند کرد.

۲ محصولات تحت تأثیر

بر اساس گزارش‌های منتشر شده، روترهای DAP-1522 و DIR-816L که از جانب شرکت D-Link پشتیبانی نمی‌شوند، تحت تأثیر این آسیب‌پذیری‌ها قرار دارند. این دستگاه‌ها، فریمورهای نسخه v1.42 و v12.06.B09 و قبل‌تر را اجرا می‌کنند و در حال حاضر بروزرسانی‌های امنیتی منتشر شده را دریافت نخواهند کرد.

۳ جزئیات فنی و روش‌های بهره‌برداری

آسیب‌پذیری‌های مورد بحث، توسط تیم ACE، از شرکت Loginsoft گزارش داده شده‌اند که در ادامه در خصوص جزئیات فنی هر یک از آن‌ها بیشتر توضیح داده خواهد شد، گفتنی است که برخی از این نقص‌ها در ۹ فوریه ۲۰۱۹ و برخی دیگر نیز در مارس ۲۰۲۰ گزارش داده شدند؛ اما همه آن‌ها در ۲۲ جولای ۲۰۲۰ به طور عمومی منتشر شدند.

۱. CVE-2020-15892

این نقص یک آسیب‌پذیری سرریز بافر مبتنی بر پشته کلاسیک در D-LINK Firmware DAP 1520 می‌باشد که شدت بحرانی و Base Score 9.8 به آن اختصاص داده شده است.

---

[۱] End-of-Support

[۲] End-of-Life

Extender یک گسترش‌دهنده محدوده وایرلس قابل حمل[۳] است که به کاربران امکان می‌دهد منطقه پوشش شبکه وایرلس موجود را توسعه و گسترش دهند. کاربران می‌توانند برای افزایش دامنه شبکه وایرلس خود آن را در هر نقطه از خانه یا محل کار قرار دهند. نسخه‌های آسیب‌پذیر Firmware، 1.0.8 و 1.10B0 هستند. این آسیب‌پذیری در D-link DAP 1520 access point، در binary ‘ssi’ وجود دارد و منجر به اجرای دستورات دلخواه می‌شود. زمانیکه که کاربر از طریق رابط وب اقدام به ورود به سیستم می‌کند، مقادیر درخواست به ‘ssi’ binary ارسال می‌شوند. در صفحه ورود، رابط وب طول ورودی رمزعبور را به ۱۵ کاراکتر محدود می‌کند. مشکل ناشی از آن است که اعتبارسنجی کاربر از طرف کلاینت انجام می‌شود، از این جهت زمانیکه یک مهاجم موفق به رهگیری درخواست ورود به سیستم (POST based) می‌شود و از پارامتر آسیب‌پذیر (`log_pass`) برای افزایش طول رمزعبوراستفاده کند، این اعتبارسنجی می‌تواند دور زده شود و درخواست به وب سرور ارسال گردد. تعداد کمی از متغیرهای POST که به عنوان بخشی از درخواست ورود به سیستم منتقل می‌شوند، آسیب‌پذیر هستند که عبارتند از: `html_response_page` و `log_user`. جهت رفع و یا کاهش اثر این آسیب پذیری می‌توان طول رمزعبور باید در سمت سرور بررسی شود و در صورت عدم اعتماد به ورودی، حافظه باید به صورت پویا تخصیص یابد.

۲. CVE-2020-15893:

این نقص یک آسیب‌پذیری تزریق دستور در روترهای DIR-816L با شدت بحرانی و Base Score 9.8 است که به مهاجم اجازه می‌دهد از طریق یک پکت جعلی M-SEARCH، دستورات دلخواه خود را به UPnP تزریق کند. Universal Plug and Play (UPnP) به طور پیش‌فرض در DIR-816L و در پورت ۱۹۰۰ فعال شده است. مهاجم می‌تواند این حمله را با تزریق پی‌لود در قسمت (ST) ‘Search Target` مربوط به SSDP M-SEARCH discover packet انجام دهد. جهت رفع و یا کاهش اثر این آسیب پذیری برای فیلترکردن پی‌لودهای مرتبط به تزریق دستور، از روش لیست سیاه یا Blacklist استفاده شود، مانند `;`، `||` و غیره.

۳. CVE-2020-15894:

این نقص در روترهای DIR-816L با شدت بالا و با Base Score 7.5 اعلام شده است. در بهره‌برداری از این آسیب‌پذیری مهاجم می‌تواند هر شخصی باشد که به شبکه متصل است و همچنین قادر است به صفحه ورود روتر دسترسی داشته باشد. جهت رفع و یا کاهش اثر این آسیب پذیری قبل از هر دسترسی به عملکردهای سطح مدیریتی باید سشن به صورت درست بررسی شود.

---

[۳] portable Wireless Range Extender

۴. CVE-2020-15895:

این نقص یک آسیب‌پذیری Reflected Cross-site scripting با شدت متوسط و Base Score 6.1 در روتر DIR-816L است که ناشی از چاپ مقدار "RESULT" در صفحه وب می‌باشد. جهت رفع و یا کاهش اثر این آسیب پذیری برای حذف کاراکترهای اضافی باید جداسازی (escaping) مناسب خروجی انجام گیرد.

۵. CVE-2020-15896:

این آسیب‌پذیری با شدت بالا و Base Score 7.5 مربوط به دور زدن احراز هویت در روتر D’link DAP 1522 access point است و به مهاجم اجازه می‌دهد تا به رابط وب، دسترسی غیرمجاز پیدا کند.

۴ توصیه امنیتی

شرکت D-Link، فریمور Exceptional Beta Patch Release نسخه v1.10b04Beta02 را برای مدل D-Link DAP-1520 که فریمور آسیب‌پذیر نسخه v1.10B04 را اجرا می‌کنند، منتشر کرد. لذا با توجه به اهمیت آسیب‌پذیری‌های مذکور و بالا بودن شدت آن‌ها، هرچه سریع‌تر نسبت به وصله این آسیب‌پذیری‌ها، اقدام کنید.

۵ منابع

[1] https://securityaffairs.co/wordpress/106351/hacking/d-link-flaws.html

[2] https://research.loginsoft.com/vulnerability/classic-stack-based-buffer-overflow-in-dlink-firmware-dap-1520/

[3] https://research.loginsoft.com/vulnerability/multiple-vulnerabilities-discovered-in-the-d-link-firmware-dir-816l/

[4] https://research.loginsoft.com/vulnerability/authentication-bypass-in-d-link-firmware-dap-1522/