بسمه‌تعالی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر
مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

به‌روزرسانی محصولات سیسکو

خبر به‌روزرسانی

شناسه سند	MaherReporte_13991121-01
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۳۹۹/۱۱/۲۰
طبقه‌بندی سند	عادی

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ به‌روزرسانی محصولات سیسکو

شرکت سیسکو برای چندین آسیب‌پذیری بحرانی (CVE-2021-1289 تا CVE-2021-1295) موجود در روترهای web-based management interface of Small Business سری RV160، RV160W، RV260، RV260P و RV260W VPN نسخه‌های پیش از ۱،۰،۰۱،۰۲ به‌روزرسانی‌هایی را منتشر کرده است. این آسیب‌پذیری‌ها به یک مهاجم غیرمجاز از راه دور امکان می‌دهد، کد دلخواه را با دسترسی root در دستگاه آسیب‌پذیر اجرا نماید. همچنین وصله هایی برای دو آسیب‌پذیریِ نوشتن فایل اختیاری (Arbitrary File Write) (CVE-2021-1296 و CVE-2021-1297) منتشر شده است که بر همان مجموعه از روترهای VPN تأثیر می‌گذارد و می‌تواند منجر به overwrite شدن فایل‌های دلخواه گردد.

آسیب‌پذیری‌های CVE-2021-1289، CVE-2021-1290، CVE-2021-1291، CVE-2021-1292، CVE-2021-1293، CVE-2021-1294 و CVE-2021-1295 به دلیل ارزیابی نامناسب درخواست‌هایHTTP وجود داشته و به مهاجم امکان می‌دهد تا یک درخواست HTTP مخرب را در رابط مدیریت مبتنی بر وب ایجاد کرده و کد دلخواه خود را در سیستم‌های آسیب‌پذیر اجرا کند.

آسیب‌پذیری‌های CVE-2021-1296 و CVE-2021-1297 به دلیل عدم ارزیابی ورودی، وجود داشته و به مهاجم امکان می‌دهد تا با بهره‌برداری از این نقص‌ها و استفاده از رابط مدیریت مبتنی بر وب، فایل دلخواه خود را در یک مکان غیرمجاز بارگذاری کند.

آسیب‌پذیری‌های CVE-2021-1314 تا CVE-2021-1318 می‌تواند به مهاجم امکان دهد تا دستورات دلخواه خود را در روترهای آسیب‌پذیر تزریق نماید. شرکت سیسکو همچنین به‌روزرسانی‌هایی برای ۳۰ آسیب‌پذیری (CVE-2021-1319 تا CVE-2021-1348) منتشر کرده است. این آسیب‌پذیری‌ها به یک مهاجم از راه دور مجاز امکان اجرای کد از راه دور و اجرای حملات انکار سرویس را می‌دهد. مهاجم جهت بهره‌برداری از این آسیب‌پذیری‌ها باید دارای اعتبارنامه‌های معتبر مدیر سیستم در دستگاه آسیب‌پذیر باشد. به گفته محققان در حال حاضر هیچ‌گونه برای بهره‌برداری فعال از این آسیب‌پذیری‌ها وجود ندارد.

جدول ۱. لیست به‌روزرسانی‌های منتشر شده

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری	شناسه آسیب‌پذیری	تاریخ انتشار آسیب‌پذیری
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	اجرای کد از راه دور	۹,۸	CVE-2021-1289	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	نوشتن فایل اختیاری (Arbitrary File Write)	۷,۵	CVE-2021-1296	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	نوشتن فایل اختیاری (Arbitrary File Write)	۷,۵	CVE-2021-1297	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	اجرای کد از راه دور	۹,۸	CVE-2021-1290	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	اجرای کد از راه دور	۹,۸	CVE-2021-1291	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	اجرای کد از راه دور	۹,۸	CVE-2021-1292	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	اجرای کد از راه دور	۹,۸	CVE-2021-1293	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	اجرای کد از راه دور	۹,۸	CVE-2021-1294	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers	اجرای کد از راه دور	۹,۸	CVE-2021-1295	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	تزریق دستور (Command Injection)	۷,۲	CVE-2021-1314	۱۵ بهمن ۱۳۹۹

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری	شناسه آسیب‌پذیری	تاریخ انتشار آسیب‌پذیری
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	تزریق دستور (Command Injection)	۷,۲	CVE-2021-1318	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1319	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	تزریق دستور (Command Injection)	۷,۲	CVE-2021-1315	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	تزریق دستور (Command Injection)	۷,۲	CVE-2021-1316	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	تزریق دستور (Command Injection)	۷,۲	CVE-2021-1317	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1320	۱۵ بهمن ۱۳۹۹

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری	شناسه آسیب‌پذیری	تاریخ انتشار آسیب‌پذیری
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1321	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1322	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1323	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1324	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1325	۱۵ بهمن ۱۳۹۹

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری	شناسه آسیب‌پذیری	تاریخ انتشار آسیب‌پذیری
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1326	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1327	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1328	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1329	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1330	۱۵ بهمن ۱۳۹۹

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری	شناسه آسیب‌پذیری	تاریخ انتشار آسیب‌پذیری
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1331	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1332	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1333	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1334	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1335	۱۵ بهمن ۱۳۹۹

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری	شناسه آسیب‌پذیری	تاریخ انتشار آسیب‌پذیری
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1336	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1337	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1338	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1339	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1340	۱۵ بهمن ۱۳۹۹

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری	شناسه آسیب‌پذیری	تاریخ انتشار آسیب‌پذیری
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1341	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1342	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1343	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1344	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1345	۱۵ بهمن ۱۳۹۹

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری	شناسه آسیب‌پذیری	تاریخ انتشار آسیب‌پذیری
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1346	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1347	۱۵ بهمن ۱۳۹۹
Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers	اجرای کد از راه دور (Remote Command Execution) و انکار سرویس (Denial of Service)	۷,۲	CVE-2021-1348	۱۵ بهمن ۱۳۹۹

منبع

https://threatpost.com/cisco-flaws-vpn-routers-rce/163662/