شنبه 18 فروردین 1397 - 11:35

مرکز ماهر منتشر کرد : جزئیات حمله سایبری به دیتاسنترهای کشور

مرکز ماهر اعلام کرد: بروز اختلالات سراسری در سرویس اینترنت و سرویس‌های مراکز داده داخلی ناشی از حمله به تنظیمات تجهیزات روتر و سوئیچ متعدد شرکت سیسکو بوده است.

شب گذشته هکرها با سوءاستفاده از یک آسیب پذیری در کلاینت اسمارت اینستال شرکت سیسکو موفق به نفوذ در زیرساخت های مهم دیجیتال در برخی کشورها و از جمله ایران شدند که منجر به بروز اختلالاتی سراسری در سرویس اینترنت و سرویس های مراکز داده داخلی شد.

در همین ارتباط مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای (ماهر) اطلاعیه ای منتشر و اعلام کرده است که در پی بروز اختلالات سراسری در سرویس اینترنت و سرویس های مراکز داده داخلی در ساعت حدود 20:15 در تاریخ هفدهم فروردین ماه 97 بررسی و رسیدگی فنی به موضوع انجام و مشخص شد این حملات شامل تجهیزات روتر و سوئیچ متعدد شرکت سیسکو بوده که تنظیمات این تجهیزات مورد حمله قرار گرفته و کلیه پیکربندی های این تجهیزات (شامل running-config و startup-config) حذف گردیده است.

در موارد بررسی شده پیغامی با این مضمون در غالب startup-config مشاهده گردید: دلیل اصلی مشکل، وجود حفره امنیتی در ویژگی smart install client تجهیزات سیسکو بوده و هر سیستم عاملی که این ویژگی بر روی آن فعال باشد در معرض آسیب پذیری مذکور قرار داشته و مهاجمین می توانند با استفاده از اکسپلویت منتشر شده نسبت به اجرای کد از راه دور بر روی روتر/سوئیچ اقدام کنند.

لازم است مدیران سیستم با استفاده از دستور "no vstack" نسبت به غیرفعال سازی قابلیت فوق (که عموماً مورد استفاده نیز قرار ندارد) بر روی سوئیچ ها و روترهای خود اقدام کنند، همچنین بستن پورت 4786 در لبهٔ شبکه نیز توصیه می شود. در صورت نیاز به استفاده از ویژگی smart install، لازم است به روزرسانی به آخرین نسخه های پیشنهادی شرکت سیسکو صورت پذیرد.

جزییات فنی این آسیب پذیری و نحوهٔ برطرف سازی آن در منابع زیر آمده است:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2#fixed

در این راستا به محض شناسایی عامل این رخداد، دسترسی به پورت مورد استفاده توسط اکسپلویت این آسیب پذیری در لبه شبکه زیرساخت کشور و همچنین کلیه سرویس دهنده های عمدهٔ اینترنت کشور مسدود شد.

ماهر اعلام کرده است که تا این لحظه، سرویس دهی شرکت ها و مراکز داده بزرگ از جمله افرانت، آسیا تک، شاتل، پارس آنلاین و رسپینا بصورت کامل به حالت عادی بازگشته و اقدامات لازم جهت پیشگیری از تکرار رخداد مشابه انجام شده است.

همچنین لازم به توضیح است متاسفانه ارتباط دیتاسنتر میزبان وب سایت مرکز ماهر نیز دچار مشکل شده بود که در ساعت ۴ بامداد مشکل حل شد. همچنین پیش بینی می شود که با آغاز ساعت کاری سازمان ها، ادارات و شرکت ها، شمار قابل توجهی از این مراکز متوجه وقوع اختلال در سرویس شبکه داخلی خود شوند. لذا مدیران سیستم های آسیب دیده لازم است اقدامات زیر را انجام دهند: با استفاده از کپی پشتیبان قبلی، اقدام به راه اندازی مجدد تجهیز خود کنند یا در صورت عدم وجود کپی پشتیبان، راه اندازی و تنظیم تجهیز مجدداً انجام پذیرد.

قابلیت آسیب پذیر smart install client را با اجرای دستور "no vstack" غیر فعال گردد. لازم است این تنظیم برروی همه تجهیزات روتر و سوئیچ سیسکو (حتی تجهیزاتی که آسیب ندیده اند) انجام شود و رمز عبور قبلی تجهیز تغییر داده شود.

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای (ماهر) در پایان توصیه کرده است که در روتر لبه شبکه با استفاده از ACL ترافیک ورودی TCP 4786 نیز مسدود شود. ضمن اینکه متعاقبا گزارشات تکمیلی در رابطه با این آسیب پذیری و ابعاد تاثیرگذاری آن در کشور و سایر نقاط جهان را منتشر خواهد کرد.

هیچ دسترسی غیرمجازی به اطلاعات شهروندان اتفاق نیفتاده است

در این باره، سرهنگ علی نیک نفس، رئیس مرکز تشخیص سایبری با اشاره به حمله سایبری شب گذشته اظهار کرد: این حملات ناشی از آسیب پذیری در قابلیت پیکربندی راه دور تجهیزات سیسکو بوده است. این آسیب پذیری حدود ۱۰ روز قبل توسط این شرکت اعلام و رسانه ای شده بود که اطلاعات آن در سایت پلیس فتا و مرکز ماهر موجود است.

به گزارش ایسنا، نیک نفس با بیان اینکه مشکلی که به وجود آمده، صرفاً به خاطر از کار افتادن سوئیچ های در شبکه هاست تصریح کرد: طبیعی است این اختلال قطعی و کندی اینترنت را برای کاربران شرکت ها در پی داشته است اما هیچ نوع دسترسی غیرمجاز و یا نشر اطلاعات رخ نداده است و ازاین جهت جای نگرانی وجود ندارد.

رئیس مرکز تشخیص سایبری که در یک برنامه تلویزیونی سخن می گفت، با بیان اینکه این شرکت ها باید سعی کنند تا اختلالات موجود را حل کنند، گفت: این اختلالات حل شده و تا حدی روی سرویس های اصلی اینترنتی کشور برطرف شده است اما با توجه به ساعات ابتدایی کاری این هفته برخی از شرکت ها احتمالاً متوجه اختلالات در شبکه خود خواهند شد که باید نسبت به آسیب پذیری و رفع مشکل اقدام کنند.

<form/>