اشتباه نابخشودني دانشگاه مينه‌سوتا چه بود که باعث شد به‌طور کامل از پروژه‌ي بزرگ کرنل لينوکس کنار گذاشته شود؟ در اين مقاله ابعاد اين ماجرا را بررسي مي‌کنيم.

عصر روز ششم آوريل ، يکي از دانشجويان دانشگاه مينه‌سوتا پَچي مربوط به پروژه‌ي کرنل لينوکس را به چند توسعه‌دهنده ايميل کرد. پانزده روز بعد، اين دانشگاه که همواره جزو مؤسسه‌ي تحقيقاتي برتر دنيا بوده است، از شرکت در اين پروژه‌ي مهم و بزرگ به‌طور کامل کنار گذاشته شد.

گرِگ کروآ هارتمن، يکي از توسعه‌دهندگان ارشد و نگهدارنده‌ي کرنل لينوکس، در جواب اين ايميل با عصبانيت نوشت: «من به شما پيشنهاد مي‌کنم براي انجام آزمايش‌هايتان سراغ انجمن ديگري برويد. اينجا ديگر جاي شما نيست.»

گرِگ هارتمن: اينجا ديگر جاي شما نيست

اما چه شد که تنها يک ايميل باعث ممنوعيت کل يک دانشگاه از شرکت در پروژه‌ي کرنل لينوکس شد؟ پروژه‌ي متن بازي که با داشتن بيش از ميليون خط کد از هزاران توسعه‌دهنده، بزرگ‌ترين پروژه‌ي حوزه‌ي نرم‌افزار در دنيا محسوب مي‌شود و توسعه‌دهندگان بسياري اين همکاري داوطلبانه را افتخار بزرگي براي خود مي‌دانند.

براي خواندن داستان پرفرازونشيب مشارکت اين دانشگاه در پروژه‌ي کرنل لينوکس و دليل کنار گذاشته شدن آن از اين پروژه، با ما همراه باشيد.

داستان از سال شروع شد؛ يعني زماني‌که يک محقق امنيت سيستم به نام کنگجي لو استاديار دانشگاه مينه‌سوتا شد.

تحقيقات لو، طبق چيزي که در وب‌سايت او نوشته شده، در مورد «تقاطع امنيت، سيستم عامل‌‎ها، تجزيه و تحليل برنامه و کامپايلرها» است؛ اما لو توجهش معطوف به لينوکس بود و بيشتر مقاله‌هاي او به‌نوعي مربوط به کرنل لينوکس است.

مقاله‌ي مرتبط:

کرنل و عملکرد آن چيست؟

هسته يا کرنل لينوکس هسته‌ي اصلي هر سيستم عامل لينوکس است و در واقع رابطي بين سيستم عامل و دستگاهي است که سيستم عامل روي آن اجرا مي‌شود. يک کاربر لينوکس هيچ تعاملي با هسته ندارد؛ اما وجود آن براي انجام کارهاي مختلف، از جمله مديريت حافظه، مديريت ديسک و پردازنده،‌ ضروري است.

کرنل لينوکس پروژه‌اي متن باز است، به اين معني که ميليون‌ها خط کد آن در دسترس عموم است و همه مي‌توانند آن‌ها را ببينند و کدهاي خود را به آن اضافه کنند.

البته نه «همه» چون قرار نيست هر پچي که به توسعه‌دهندگان پروژه ارسال مي‌شود، مورد تأييد قرار بگيرد و به کامپيوتر ميليون‌ها کاربر در دنيا راه پيدا کند. هر پچ ارسال‌شده ابتدا بايد از نظارت شبکه‌ي گسترده‌اي از توسعه‌دهندگان و «نگهدارندگان»‌ (هزاران داوطلب که هر يک مسئول نگه‌داري از اجزاي مختلف هسته است)‌ بگذرد تا بتواند در مخزن اصلي قرار گيرد.

کانجي لو پروفسور دانشگاه مينه سوتا

داستان از سال شروع شد: زماني‌ که کنگجي لو به‌عنوان استاديار دانشگاه مينه‌سوتا شروع به کار کرد.

وقتي پچ به اين مرحله رسيد، تازه بايد يک دوره‌ آزمايش طولاني‌مدت را پشت سر بگذارد تا براي گنجانده شدن در «عرضه‌ي پايدار»‌ و سيستم‌هاي عامل‌ کاربران مورد تأييد قرار بگيرد. اين فرايند به اين دليل اين‌چنين سختگيرانه طراحي‌ شده است تا از ورود کدهاي مخرب يا بي‌کيفيت جلوگيري کند؛ اما ماهيت متن باز بودن اين پروژه هميشه جايي براي خطاي انساني باز مي‌گذارد.

برخي از پروژه‌هاي اخير لو مرتبط با خطاي انساني و کاهش اثرات آن بوده است. او با آزمايش کرنل لينوکس،‌ سيستم‌هايي را براي تشخيص خودکار انواع مختلف باگ‌ها در پروژه‌هاي متن باز معرفي کرده است. اين آزمايش‌ها شامل گزارش باگ، ارسال پچ به نگهدارندگان کرنل لينوکس و گزارش نرخ پذيرفته شدن پچ‌هاي او توسط نگهدارندگان است.

با هدف گرفتن انجمن کرنل لينوکس دردسرها شروع شد

براي مثال، لو و دو نفر از دانشجويان دکتراي او به نام‌هاي آديتيا پکي و چيوشي وو در مقاله‌اي در سال ???? سيستمي به نام کريکس (Crix) را براي تشخيص دسته‌ي خاصي از باگ‌ها در هسته‌هاي سيستم عامل ارائه دادند. اين سه نفر، ??? مورد از اين باگ‌ها را به کمک کريکس پيدا کردند و براي رفع همه‌ي آن‌ها پچ‌هايي ارسال کردند. اينکه نگهدارندگان وجود ??? مورد از اين باگ‌ها را تأييد کردند، گواه بر عملکرد قابل قبول اين ابزار بود.

پژوهش‌هاي لو مفيد بود؛ تا اينکه اواخر سال گذشته، لو تمرکز پژوهش‌هاي خود را از روي هسته برداشت و به انجمن توسعه‌دهندگان آن منعطف کرد و دردسرها از همين‌جا شروع شد.

لو و وو در مقاله‌اي با عنوان «امکان وارد کردن مخفيانه‌ي آسيب‌پذيري‌ها در نرم‌افزار متن باز از طريق کاميت‌هاي فريبنده» توضيح دادند که با ارسال پچ‌هايي که در ظاهر به نظر مي‌رسيد قرار است باگ‌هاي واقعي را برطرف کنند،‌ توانستند باگ‌هاي جديد و خطرناکي را به کرنل لينوکس وارد کنند. اين گروه، نام اين پچ‌ها را به خاطر ظاهر مفيد اما ماهيت مخرب آن‌ها، «کاميت‌هاي فر گذاشت.

هدف از اين آزمايش، به گفته‌ي خود اين محققان، بهبود امنيت کرنل لينوکس از طريق نشان دادن راه‌هاي نفوذ يک کدنويس مخرب به اين پروژه بود. شايد بتوان گفت روش کار آن‌ها شبيه هکرهاي اخلاقي يا همان هکرهاي کلاه سفيد است که براي کشف نقاط ضعف سيستم با شرکتي قرارداد مي‌بندند و به محض پيدا کردن باگ‌هاي نرم‌افزار، توسعه‌دهندگان را در جريان آن‌ها قرار مي‌دهند.

اما پرسروصداترين واکنشي که اين مقاله در توييتر و انجمن توسعه‌دهندگان لينوکس دريافت کرد، نه از روي قدرداني که اعتراضي کوبنده بود. برخي، از جمله گرِگ اسکات، متخصص فناوري اطلاعات با بيش از ?? سال تجربه‌ي کار با نرم‌افزار متن باز، اين مقاله را «سراسر جفنگ» ناميدند و عده‌اي ديگر، از جمله کنث وايت، محقق امنيتي، کار اين گروه را «کاملا غير اخلاقي»‌ دانستند.

پچ‌هاي لو ظاهري مفيد اما ماهيتي مخرب داشتند

البته اين عصبانيت‌ها به خاطر وجود خود اين کاميت‌ها نبود؛ چون طبق ادعاي لو، هيچ کدام از باگ‌هاي آن‌ها به کرنل لينوکس راه پيدا نکرده بود و آن‌ها خودشان اين باگ‌ها را پيش از اين مرحله حذف کرده و پچ‌هاي واقعي را به‌جاي آن‌ها ارسال کردند (اگرچه به گفته‌ي کروآ هارتمن، يکي از اين پچ‌هاي مشکل‎‌دار وارد مخزن اصلي شد؛ اما آسيبي وارد نکرد).

دليل اصلي اين واکنش‌هاي تند و انتقادي به آزمايش لو، وقت ارزشمند نگهدارندگاني بود که اين دانشگاه به‌طور عامدانه تلف کرده بود. هکرهاي کلاه سفيد با آگاهي کامل توسعه‌دهندگان دست به آزمايش و دست‌کاري سيستم مي‌زنند؛ اما پژوهش لو کاملا مخفيانه صورت گرفته است.

اسکات در اين رابطه به گفت:‌ «اين پژوهشگران از خطي که نبايد عبور کردند. هيچ کس اين گروه را براي اين کار استخدام نکرده بود. آن‌ها خودشان تصميم به انجام اين آزمايش گرفتند و افراد زيادي براي ارزيابي پچ‌هاي آن‌ها وقت گذاشتند.»

به گفته‌ي اسکات، هيچ داوطلبي از اينکه بفهمد وقت خود را براي ارزيابي پچي هدر داده که بخشي از انجام آزمايش بوده، خوشحال نخواهد بود.

دانشگاه مينه سوتا

دانشگاه مينه‌سوتا براي جلب اعتماد تيم کرنل لينوکس راه درازي در پيش دارد

از طرف ديگر، پژوهش لو پاي بحث جنجالي آزمايش انساني را نيز به ميان کشيده است. دانشگاه مينه‌سوتا معتقد است اين مسئله در مورد لو و دستيارانش وارد نيست؛ چون آن‌ها در پاسخ به اين اعتراض، تأييديه درخواست کرده بودند و نامه‌ي رسمي معافيت آن‌ها اعطا شده بود؛ اما اعضاي انجمن توسعه‌ي کرنل لينوکس چنين اعتقادي ندارند.

مقاله‌ي مرتبط:

تيم لينوکس کرنل عذرخواهي دانشگاه مينه‌سوتا را نپذيرفت

به گفته‌ي هارتمن، «پژوهش روي افرادي که روحشان از اين آزمايش باخبر نيست، کار پسنديده‌اي نيست. هيچ کس از ما نپرسيد آيا انجام اين آزمايش قابل قبول است يا خير.»

توسعه‌دهندگان ديگر نيز معتقد بودند صرف‌نظر از آسيب‌ها يا فوايد حاصل از اين پژوهش، دانشگاه مينه‌سوتا نه‌تنها اعضاي انجمن کرنل لينوکس را به دردسر انداخت، بلکه فلسفه‌ي اصلي اين پروژه را نيز زير سؤال برد. هر کاربري که از سيستم عامل استفاده مي‌کند تا حدي به توسعه‌دهندگان آن سيستم اعتماد مي‌کند. اين امر خصوصاً در مورد افرادي که از نرم‌افزارهاي متن باز استفاده مي‌کنند، صادق است و برخي از کاربران لينوکس اين اصل اعتماد را بسيار جدي تلقي مي‌کنند.

اسکات در اين زمينه به گفت:

پروژه‌هاي متن باز به جامعه‌ي کاربري پرجنب‌وجوشي نياز دارند. در اين جامعه بايد افرادي براي ارسال فايل‌ها، افرادي براي مستند کردن فايل‌ها و افرادي براي استفاده از آن‌ها و ارائه‌ي بازخورد براي هرچه بهتر شدن سيستم وجود داشته باشد.

اين حلقه‌ي بازخورد به افراد زيادي وابسته است و کاربران بايد بتوانند تا حدي به اين سيستم اعتماد داشته باشند ... اگر کسي اين اعتماد را زير پا بگذارد، اوضاع به هم مي‌ريزد.

پس از انتشار مقاله، براي بسياري از توسعه‌دهندگان کرنل لينوکس روشن شد که بايد کاري در مورد دانشگاه مينه‌سوتا صورت بگيرد و تمام پچ‌هاي ارسالي از اين دانشگاه بررسي شود؛ اما روند بازبيني اين پچ‌ها در مقياس گسترده تا سال ???? محقق نشد.

روز ششم آوريل ????، آديتيا پکي با آدرس ايميل خود آن پچ سرنوشت‌ساز را به انجمن توسعه‌دهندگان کرنل لينوکس ارسال کرد.

هارتمن که از مدت‌ها به خاطر سابقه‌ي دانشگاه مينه‌سوتا در ارسال کدهاي مخرب در حالت آماده‌باش بود، با ديدن آدرس ايميل پکي تصميم گرفت همان موقع اين پچ را بررسي کند. او متوجه شد پچ ارسالي چندان مفيد به نظر نمي‌رسد. به گفته‌ي او، «بايد خيلي تلاش کرد تا پچي طراحي کرد که به نظر درست مي‌رسد؛ اما در عمل مخرب است. پچ‌هاي ارسالي دانشگاه مينه‌سوتا همه به همين شکل بودند.»

سرانجام بيستم آوريل، هارتمن تصميم گرفت با اين دانشگاه به‌طور جدي برخورد کند.

او در جواب ايميل پکي نوشت:

لطفاً از ارسال پچ‌هاي نامعتبر دست برداريد. استاد شما دارد با فرايند بازبيني بازي مي‌کند تا به روشي عجيب و غريب، مقاله بنويسد.

به گفته‌ي ليان رومانوفسکي، يکي از نگهدارندگان کرنل لينوکس، هارتمن چهار مورد از پچ‌هاي پذيرفته‌شده‌ي پکي را بررسي کرد و متوجه شد سه مورد از آن‌ها داراي آسيب‌پذيري امنيتي با درجه خطر مختلفي هستند.

هارتمن اميدوار بود داستان به همين‌جا ختم شود؛ اما پکي با عصبانيت در پيامي شخصي به او جواب داد:

با کمال احترام، از شما مي‌خواهم دست از تهمت واهي زدن و افترا برداريد.

هارتمن آوريل در جواب نوشت:

شما و تيمتان اعتراف کرديد پچ‌هاي مشکل‌دار را به انجمن کرنل فرستاده‌ايد تا واکنش آن‌ها را ببينيد و بعد بر اساس آن مقاله‌اي منتشر کرديد. حالا دوباره يک سري پچ‌ که به‌وضوح مشکل‌دار است، ارسال کرده‌ايد. انتظار داريد من درباره‌ي اين موضوع چه فکري کنم؟

هارتمن تا پايان آن روز، به‌طور رسمي در ايميلي به شماري از نگهدارندگان کرنل لينوکس و همچنين اعضاي تيم لو اعلام کرد از اين پس،‌ پچ‌هاي ارسالي با آدرس umn.edu (ايميل دانشگاه مينه‌سوتا)‌ بايد به‌طور پيش‌فرض رد شود، مگر اينکه اعتبار آن‌ها ثابت شود.

هارتمن پچ ارسالي از ايميل‌هاي وابسته به دانشگاه مينه‌سوتا را برگرداند. امکان برگرداندن پچ وجود نداشت؛ اما بايد به‌صورت دستي بررسي مي‌شدند.

پچ‌هاي دانشگاه مينه‌سوتا از اين پس به‌طور پيش‌فرض رد مي‌شود

مشخص نيست اين پچ جديد قرار بود در چه آزمايشي به کار رود. وب‌سايت لو به «پچ‌هاي اضافه‌ي آديتيا پکي براي پروژه‌ي جديد کشف باگ» اشاره‌ي کوچکي کرده است.

اما آنچه مشخص است اين است که رفتار پکي بالاخره انجمن را بر آن داشت تا در روند بررسي پچ‌هاي اين دانشگاه، هرگونه تأخير را کنار بگذارد. توسعه‌دهندگان لينوکس شروع به بررسي تمام پچ‌هايي کردند که در گذشته از ايميل‌هاي وابسته به دانشگاه مينه‌سوتا ارسال شده بودند. به‌گفته‌يجاناتان کوربت، بنيان‌گذار و. بعد از بازبيني، «بيشتر پچ‌هاي مشکوک، قابل قبول بودند؛ اما عالي نبودند.» از بيش از پچي که مشخص شده بود، مورد قرار است از هسته کنار گذاشته شوند.

خواه واکنش انجمن لينوکس به اين ماجرا موجه باشد خواه نباشد، اين انجمن بايد درباره‌ي ادامه‌ي همکاري با دانشگاه مينه‌سوتا تصميم‌گيري کند. طبق خواسته‌ي شفاف اين انجمن، اين دانشگاه بايد آن‌ها را متقاعد کند پچ‌هاي آينده قرار نيست باعث اتلاف وقت توسعه‌دهندگان شود؛ اما اين دانشگاه براي متقاعد کردن انجمن کرنل لينوکس و بازگشت به اين پروژه دقيقا بايد چه کار کند؟

درست همان روزي که دانشگاه از پروژه کنار گذاشته شد، واحد علوم کامپيوتر آن اعلام کرد تحقيقات مربوط به امنيت کرنل لينوکس را متوقف کرده و در حال پيگيري روش پژوهش لو و دستيارانش است.

اما اين براي بنياد لينوکس کافي نبود. مايک دولان، معاون ارشد بنياد لينوکس و مدير کل پروژه‌ها، در نامه‌اي به دانشگاه چهار خواسته را مطرح کرد:

دانشگاه بايد تمام اطلاعات لازم براي شناسايي تمام کدهاي آسيب‌پذير پيشنهادي را براي کمک به روند بازبيني منتشر کند.

مقاله‌ي مربوط به کاميت‌هاي فريبنده از انتشار خارج شود.

تمام آزمايش‌هاي آينده‌ي دانشگاه بايد مورد بازبيني.

اما وضعيت دانشگاه در مورد دو خواسته‌ي ديگر هنوز مشخص نيست. در نامه‌اي که واحد علوم کامپيوتر دانشگاه به بنياد لينوکس فرستاد، تأکيد شده است که هيئت بررسي نهادي دانشگاه در مورد اين قضيه کار خود را به‌درستي انجام داده است و معتقد است برداشت اين بنياد از «آزمايش انساني» با آنچه در مقررات فدرال آمريکا آمده، متفاوت است. البته در اين نامه عنوان شد دانشگاه متعهد مي‌شود آموزش‌هاي اخلاقي بيشتري براي اعضاي هيئت علمي خود در نظر بگيرد.

از آن طرف، لو و دو دستيارش در نامه‌اي سرگشاده از انجمن لينوکس عذرخواهي کردند و در عين حال به دفاع از کار خود پرداختند:

اشتباه ما اين بود که راهي براي مشورت کردن با انجمن و اجازه گرفتن از آن‌ها پيش از انجام آزمايش پيدا نکرديم. ما اين کار را به اين خاطر انجام داديم که مي‌دانستيم اگر از نگهدارندگان اجازه بگيريم، حواسشان به پچ‌هاي ما جمع مي‌شود.

آن‌ها در ادامه تکرار کردند که هيچ حفره‌ي امنيتي را به کرنل لينوکس وارد نکردند و پچ‌هاي ديگر آن‌ها هيچ ارتباطي با مطالعات آن‌ها روي کاميت‌هاي فريبنده نداشته است.

اما هارتمن گفته‌هاي آن‌ها را ناديده گرفت و تأکيد کرد تا زماني‌که آن دو خواسته‌ي ديگر محقق نشده است، هيچ حرفي بين آن‌ها باقي نمي‌ماند.

اما در اين ماجرا حق با چه کسي است؟ آيا دانشگاه مينه‌سوتا واقعا از خط قرمز عبور کرده يا بنياد لينوکس در مورد اين قضيه بيش از حد واکنش نشان داده است؟

از منظر پژوهشگران دانشگاه، هدف از اين آزمايش «سر کار گذاشتن» کسي نبوده است. آن‌ها فقط سعي داشتند مشکلي که در فرايند بازبيني نگهدارندگان کرنل لينوکس بود به آن‌ها نشان بدهند. برخي توسعه‌دهندگان اين ديدگاه دانشگاه را کاملا رد کردند و مدعي شدند اينکه فريب دادن نگهدارندگان در پروژه‌هاي متن باز ممکن است، امري کاملا بديهي است و نيازي به آزمايش و اثبات ندارد.

برخي از توسعه‌دهندگان نيز معتقدند با تمام خشمي که اين آزمايش برانگيخت، نکته‌اي که در مورد کاميت‌هاي فريبنده نشان داد، مورد قبول افراد بسياري واقع شده است.

اين ماجرا بحث‌هاي داغي در توييتر و فروم‌ها در مورد سياست‌هاي پذيرش پچ و نحوه‌ي برخورد نگهدارندگان با پچ‌هاي ارسالي از داوطلبان جديد برانگيخته است. به‌گفته‌يکريستوف هِلويگ، يکي از نگهدارنگان کرنل لينوکس:

نمايش چنين «حمله‌اي» بايد مدت‌ها پيش صورت مي‌گرفت و حالا بحث بسيار مهمي را شروع کرده است. به نظر من بايد به آن‌ها مدال افتخار داد.

کد هسته لينوکس

ماجراي دانشگاه مينه‌سوتا اطمينان برخي توسعه‌دهندگان را نسبت به امنيت اين سيستم عامل بيشتر کرده است

کاربري ديگر در پستي نوشت: «اين پژوهش به‌وضوح غير اخلاقي بود؛ اما نشان داد مدل توسعه‌ي سيستم‌هاي عامل در برابر کاميت‌هاي مخرب، آسيب‌پذير است.»

کوربت هم در پستي درباره‌ي اين حادثه خواستار بررسي بيشتر در مورد تغييرات جديد شد. اگر ما نتوانيم فرايند دقيق‌تري را نهادينه کنيم، همچنان با باگ‌هاي بسياري رو‌به‌رو خواهيم شد و اهميتي نخواهد داشت اين باگ‌ها به‌طور عامدانه وارد سيستم شده‌اند يا غير عامدانه.

برخي نيز معتقدند روشي که دانشگاه مينه‌سوتا براي اثبات آسيب‌پذيري پروژه‌ي کرنل لينوکس به کار برد، حتي براي منتقدان سرسخت آن، نکته‌ي مهمي را اثبات کرد؛ البته نکته‌اي خلاف آنچه لو و گروهش سعي در نشان دادن آن داشتند: اينکه سيستم بازبيني اين پروژه کار خود را به‌درستي انجام مي‌دهد.

اريک مينتز که مديريت ?? سرور لينوکس را در اختيار دارد، مي‌گويد اخراج دانشگاه مينه‌سوتا از پروژه‌ي کرنل لينوکس اطمينان او را به امنيت اين سيستم عامل بيشتر کرده است؛ چون اين انجمن متوجه اين قضيه شده و جلوي آن را گرفته است.

دانشگاه مينه‌سوتا براي جلب اعتماد تيم لينوکس راه درازي در پيش دارد

اسکات هم همين عقيده را دارد. از نظر او، اينکه از ادامه‌ي آزمايش‌ها اين پژوهشگران جلوگيري شد نشان‌دهنده‌ي اين است که عملکرد سيستم لينوکس دقيقا هماني است که از آن انتظار مي‌رود. «اين سيستم جواب مي‌دهد. ديديم که روش شرکت SolarWinds که پشت آن سازمان بزرگي قرار دارد، جواب نداد؛ اما اين سيستم چرا.»

اسکات به حمله‌ي سايبري گسترده به شرکت بزرگ فناوري اطلاعات آمريکايي، اشاره داشت که در آن هکرها با وارد کردن کدهاي مخرب به پچ‌هاي به‌روزرساني سيستم اين شرکت، ماه‌ها فعاليت‌هاي کارکنان اين شرکت را بدون اينکه رديابي شوند، زير نظر داشتند.

اسکات معتقد است عذرخواهي دانشگاه مينه‌سوتا صادقانه نبوده و تا زماني‌که آن‌ها واقعا از کار خود ابراز پشيماني نکرده‌اند، اعتماد دوباره‌اي بين آن‌ها شکل نخواهد گرفت. «براي جلب اعتماد ما راه درازي در پيش دارند. اميدوارم براي طي کردن اين راه آمادگي داشته باشند.»