بسمه تعالی

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

تحت تأثیر قرار گرفتن میلیاردها سیستم ویندوزی و لینوکسی توسط آسیب‌پذیری BootHole در GRUB2 Bootloader

خبر آسیب‌پذیری

شناسه سند ..... Maher_13990512-01
نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۰۵/۱۱
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

۱ خلاصه

این آسیب‌پذیری با شناسه CVE-2020-10713 و تحت عنوان BootHole، در بوت‌لودر[۱] GRUB2 وجود دارد و مهاجمان در صورت بهره‌برداری موفق از این آسیب‌پذیری می‌توانند قابلیت Secure Boot را دور بزنند و سطح دسترسی بالایی به صورت مخفیانه و ماندگار در سیستم‌های هدف به دست آورند. قابلیت Secure Boot یک ویژگی امنیتی از Unified Extensible Firmware Interface (UEFI) است که از یک بوت‌لودر برای بارگیری اجزای حساس، وسایل جانبی و سیستم‌عامل استفاده می‌کند.

۲ جزئیات فنی

آسیب‌پذیری مذکور دارای شدت ۸.۲ از ۱۰ بوده و در واقع یک آسیب‌پذیری سرریزبافر است که در GRUB2، هنگام تجزیه‌ی[۲] فایل grub.cfg رخ می‌دهد و تمام نسخه‌های GRUB2 تحت تأثیر این آسیب‌پذیری قرار دارند. این فایل پیکربندی، یک فایل خارجی بوده و در پارتیشن سیستمی EFI قرار دارد، بنابراین می‌تواند توسط مهاجم دارای سطح دسترسی مدیر بدون تغییر در عملکرد بوت‌لودرِ GRUB2، تغییر داده شود. grub.cfg یک فایل متنی بوده و همانند سایر فایل‌ها یا فایل‌های اجرایی امضاء[۳] نشده است. همین امر فرصت را برای مهاجمان فراهم می‌آورد تا مکانیسم hardware root of trust را بشکنند. در این حالت، بافر به جای متوقف کردن اجرا یا خارج شدن از فرآیند، فقط خطایی را در کنسول چاپ می‌کند و به فراخوانی تابع بازمی‌گردد. به گفته‌ی محققان، سرریز بافر به مهاجم اجازه می‌دهد امکان اجرای کد دلخواه را در محیط اجرایی UEFI به دست آورد، که این امر می‌تواند برای اجرای بدافزار، تغییر فرآیند بوت، وصله‌ی مستقیم هسته‌ی سیستم‌عامل و یا هر اقدام مخرب دیگری مورد سوءاستفاده قرار گیرد.

به منظور بهره‌برداری از آسیب‌پذیری BootHole در سیستم‌های ویندوزی، مهاجمان می‌توانند بوت‌لودرهایِ پیش‌فرضِ نصب شده بر روی سیستم را با یک نسخه آسیب‌پذیر GRUB2، جهت نصب بدافزار rootkit جایگزین کنند. همانطور که در تصویر ۱ قابل مشاهده است، محتوای grub.cfg از دیسک به بافر هیپ خوانده شده و سپس توسط کد آسیب‌پذیر تجزیه می‌شود که در نتیجه موجب سرریز ساختار تجزیه‌گر[۴] داخلی می‌گردد.

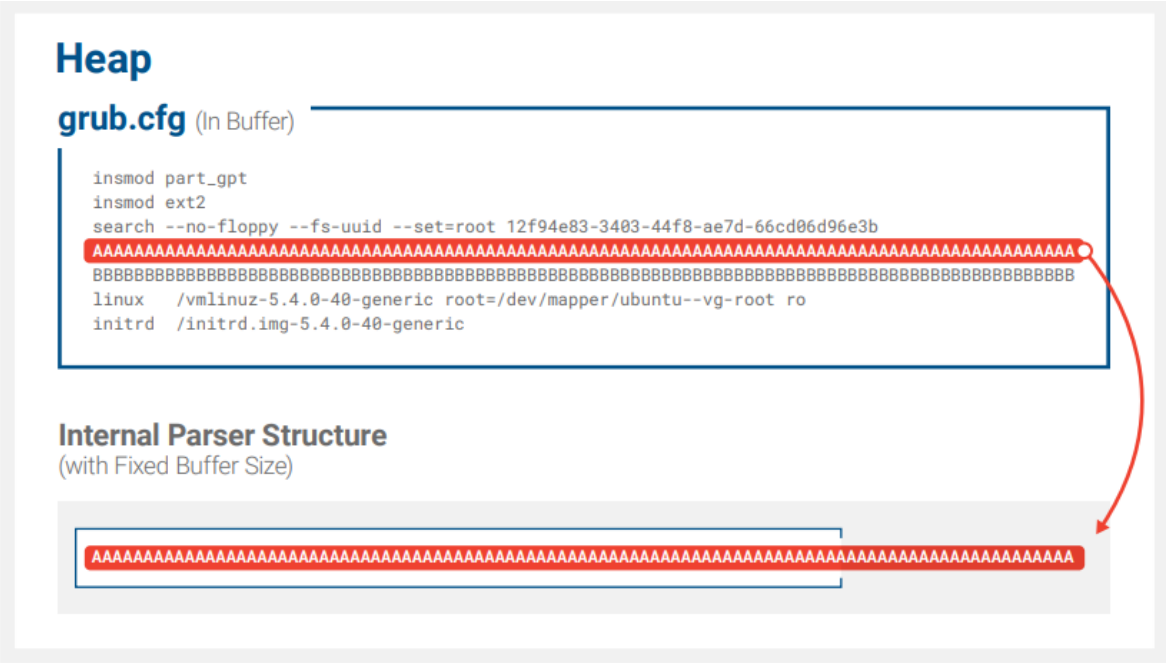
---

[۱] bootloader

[۲] parse

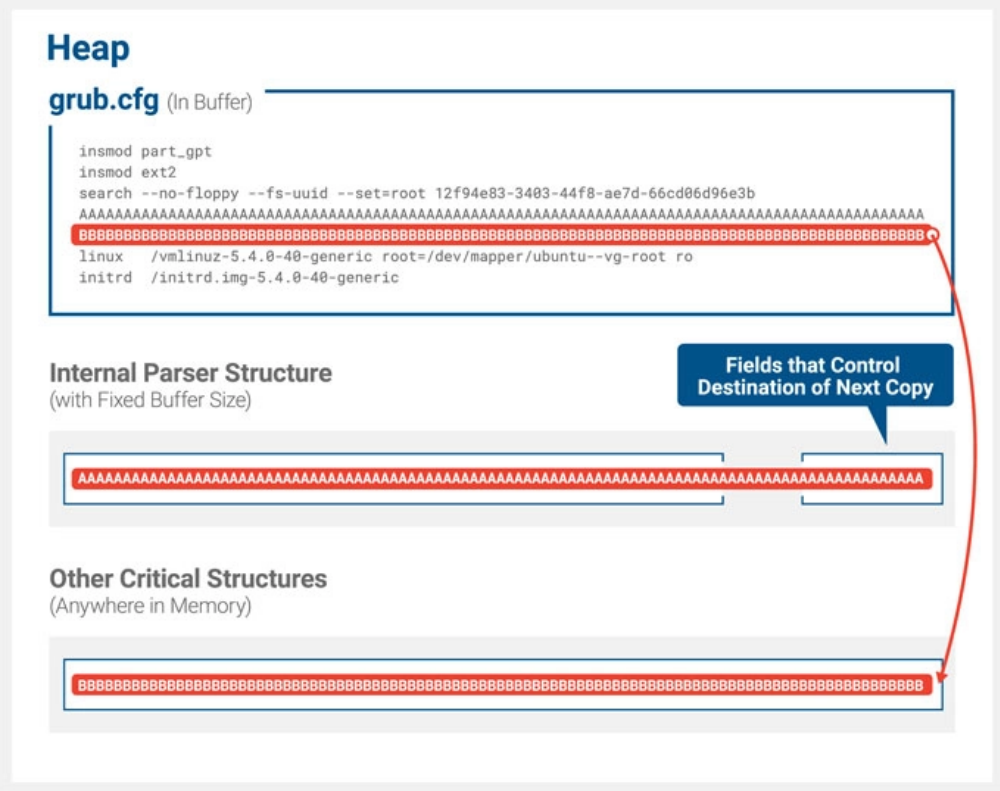
[۳] sign

[۴] parser



تصویر ۱ سرریز بافر در ساختار تجزیه‌گر داخلی

همچنین مطابق آنچه در تصویر ۲ آمده است، فیلدهای موجود در ساختار تجزیه‌گر داخلی بازنویسی شده و امکان نوشتن داده‌ی دلخواه در هر بخش از حافظه امکان‌پذیر می‌گردد.



تصویر ۲ بازنویسی فیلدهای تجزیه‌گر داخلی جهت نوشتن داده‌ی دلخواه

لازم به ذکر است که این آسیب‌پذیری از راه دور قابل بهره‌برداری نبوده و مهاجم باید پیش از هر چیز ابتدا راه نفوذی به سیستم هدف بیابد و بتواند سطح دسترسی خود را به Admin یا root ارتقاء دهد، تا بتواند از آسیب‌پذیری مذکور سوءاستفاده کند. از طرف دیگر مهاجم باید دسترسی فیزیکی به سیستم هدف داشته باشد.

۳ نسخه‌های تحت تأثیر آسیب‌پذیری

این آسیب‌پذیری میلیاردها دستگاه در سراسر جهان (از جمله سرورها و ایستگاه‌های کاری، لپ‌تاپ‌ها، دسکتاپ‌ها و سیستم‌های IoT و تقریباً هر سیستم لینوکسی و ویندوزی) را تحت تأثیر قرار می‌دهد. اگرچه GRUB2 یک بوت‌لودر استاندارد است که توسط اکثر سیستم‌های لینوکسی مورد استفاده قرار می‌گیرد، اما سیستم‌عامل‌های دیگر، هسته‌ها و هایپروایزرهایی نظیر XEN را نیز پشتیبانی می‌کند. همچنین این مشکل برای هر دستگاه ویندوزی که از Secure Boot با استاندارد Microsoft Third Party UEFI Certificate Authority استفاده می‌کند قابل تعمیم است.

۴ راهکار

نظارت بر محتوای پارتیشن بوت‌لودر (پارتیشن سیستمی EFI) می‌تواند در شناسایی زودهنگام سیستم‌های آسیب‌دیده در سازمان کمک‌کننده باشد. راه‌حل‌های زیر جهت کاهش و رفع آسیب‌پذیری پیشنهاد می‌گردد:

- به‌روزرسانی GRUB2 جهت رفع آسیب‌پذیری.
- به‌روزرسانی installers، bootloaders و shims در تمام نسخه‌های لینوکس و سایر محصولاتی که از GRUB2 استفاده می‌کنند.
- امضاء shimsهای جدید توسط صادرکنندگان گواهی UEFI شخص ثالث مایکروسافت.
- نصب نسخه‌ی جدید سیستم‌عامل در دستگاه‌های آسیب‌پذیر.
- به‌روزرسانی لیست ابطال UEFI (dbx) در سیستم‌عامل دستگاه‌های آسیب‌پذیر جهت جلوگیری از اجرای کد هنگام بوت شدن سیستم.
- جایگزین نمودن بوت‌لودرهای جدید با بوت‌لودرهای قدیمی و ابطال بوت‌لودرهای قدیمی و آسیب‌پذیر جهت جلوگیری از سوءاستفاده مهاجمان.

۵ منابع

[1] https://thehackernews.com/2020/07/grub2-bootloader-vulnerability.html?m=1
[2] https://eclypsium.com
[3] https://www.helpnetsecurity.com/2020/07/30/cve-2020-10713/