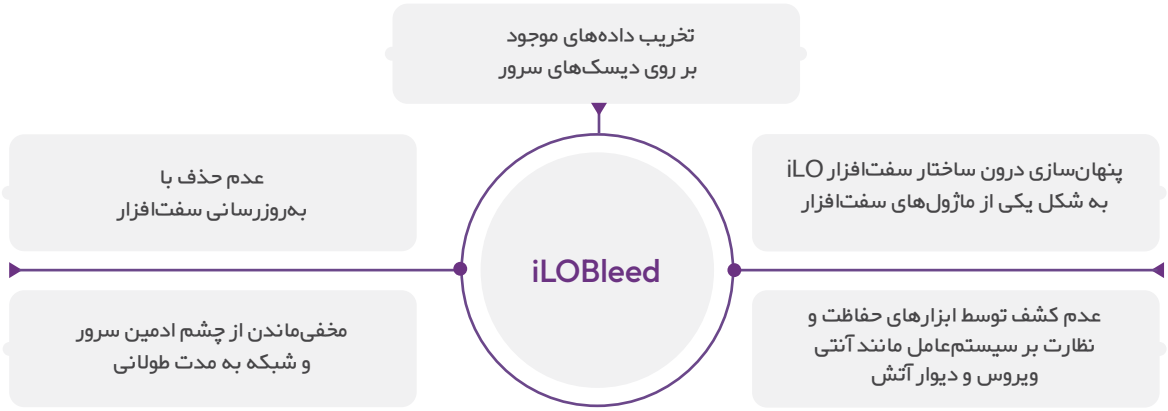
Amnpardaz®
Software Corporation

Padvish
iLO Scanner

چالش ها

نهان افزار iLO Bleed چیست؟

کشف اولین نمونه از نهان‌افزار (rootkit) در سفت‌افزار iLO سرورهای HP با نام Implant.ARM.iLOBleed.a توسط گروه تحلیل بدافزار شرکت نرم‌افزاری امن‌پرداز



ویژگی‌های ماژول iLO

ماژول (Integrated Lights-Out) iLO در سرورهای HP به مثابه بهشت نفوذگران و گروه‌های APT

۱	این ماژول به محض اتصال جریان برق به سرور، روشن می‌شود
۲	با خاموش شدن سرور (عدم قطع جریان برق) باز هم به کار خود ادامه می‌دهد
۳	دسترسی فوق‌العاده بالای این ماژول به کل سفت‌افزار، سخت‌افزار، نرم‌افزار و سیستم‌ـ عامل سرور (بالاتر از هر سطح دسترسی در سیستم‌عامل یا هایپروایزر سرور)
۴	عمومی نبودن دانش و ابزارهای لازم برای بررسی و محافظت آن برای ادمین‌های شبکه
۵	ثابت بودن و عدم تغییر آن حتی با تغییر سیستم‌عامل
۶	اجازه دسترسی کامل ادمین به کنسول مدیریتی سرور برای خاموش یا روشن کردن و نصب سیستم‌عامل روی سرور از راه دور

تأثیر تجاری و فنی این چالش‌ها

- تحمیل خسارات مادی و معنوی به اعتبار فنی و تجاری سازمان‌ها و شرکت‌های دولتی و خصوصی
- خرابکاری و توقف خدمات از طریق حذف کلیه داده‌ها و سرویس‌های مستقر روی سرورهای مراکز زیرساختی
- جاسوسی از داده‌های محرمانه مراکز حساس امنیتی، نظامی، صنعتی و ...
- ایجاد ضربات جبران ناپذیر به امنیت ملی و حاکمیت کشور در صورت گسترش حملات

راه‌حل

راهکار

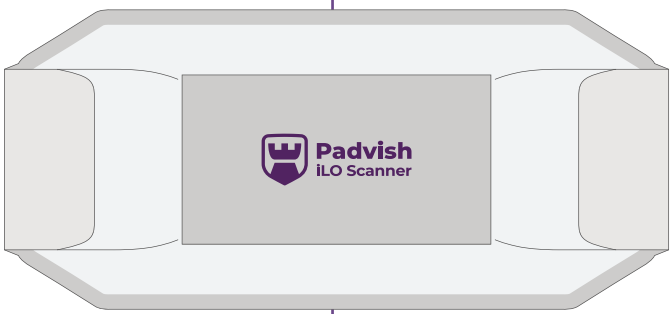
پایش دقیق سفت‌افزار iLO با ابزار تخصصی و مطمئن جهت یافتن هرگونه آلودگی

طراحی و پیاده‌سازی دستگاه Padvish iLO Scanner در شرکت نرم‌افزاری امن‌پرداز
با بهره‌گیری از دانش فنی و تجربه میدانی

فرآیند طراحی و پیاده‌سازی دستگاه

- طراحی رابط کاربری دیجیتال
- توسعه نرم‌افزار
- مهندسی معکوس
- تحلیل سفت‌افزار

معماری دستگاه Padvish iLO Scanner



- گیره اختصاصی برای اتصال مستقیم به انواع تراشه‌های SMD NOR Flash 8 و 16 پایه
- واسط کاربری لمسی خازنی 4.3"
- پردازنده مرکزی STM32F با فرکانس کاری 180MHz
- دارای دو ماژول باتری (7.4 V ,2000 mAh) با قابلیت عملکرد مستمر بیش از 6 ساعت
- پشتیبانی از ماژول SD Card برای ذخیره گزارشات

راه‌حل

ویژگی‌های کلیدی و قابلیت‌های کلی

- **پایش مستقیم سفت افزار iLO سرورهای HP**
  - پشتیبانی از نسل ۸ تا ۱۱ سرورهای HP
  - تهیه رونوشت از سفت‌افزار با دسترسی مستقیم به تراشه در وضعیت سرور خاموش
  - ارائه گزارش وضعیت اصالت و امنیت نسخه سفت‌افزار iLO نصب شده روی سرور با الگوریتم منحصر به فرد

- **حذف آلودگی‌های احتمالی و رفع تهدیدات امنیتی**
  - قابلیت پاک سازی بدافزارهای احتمالی موجود در سفت افزار iLO (iLOBleed) و ...
  - امکان به‌روزرسانی نسخه سفت‌افزار به آخرین نسخه معتبر ارائه شده توسط شرکت HP

- **پیشرفته و ایمن**
  - دسترسی به محتوای تراشه NOR Flash بدون نیاز به خارج کردن سرور از RACK و جداسازی قطعه‌ای از برد سرور
  - سرعت بالای انتقال داده و جبران اثرات لودینگ (سلفی و خازنی) مدار بار
  - دارای مدار هوشمند با جبران اثر لودینگ(سلفی و خازنی) مداربار و هشدار اتصال اشتباه گیره به کاربر و قطع جریان جهت جلوگیری اتصال کوتاه در مدار سرور

سایر ویژگی‌ها

- تشخیص، شرکت سازنده سری ساخت و حجم تراشه NOR Flash پس از اتصال گیره و قبل از شروع پایش
- هشدار خرابی چیپ
- امکان پاک‌سازی سفت‌افزارهای آلوده و به‌روزرسانی سرور به آخرین نسخه منتشرشده توسط شرکت HP
- نمایش فایل‌های موجود در SD Card متصل شده به دستگاه (File Explorer)

روش عملکرد

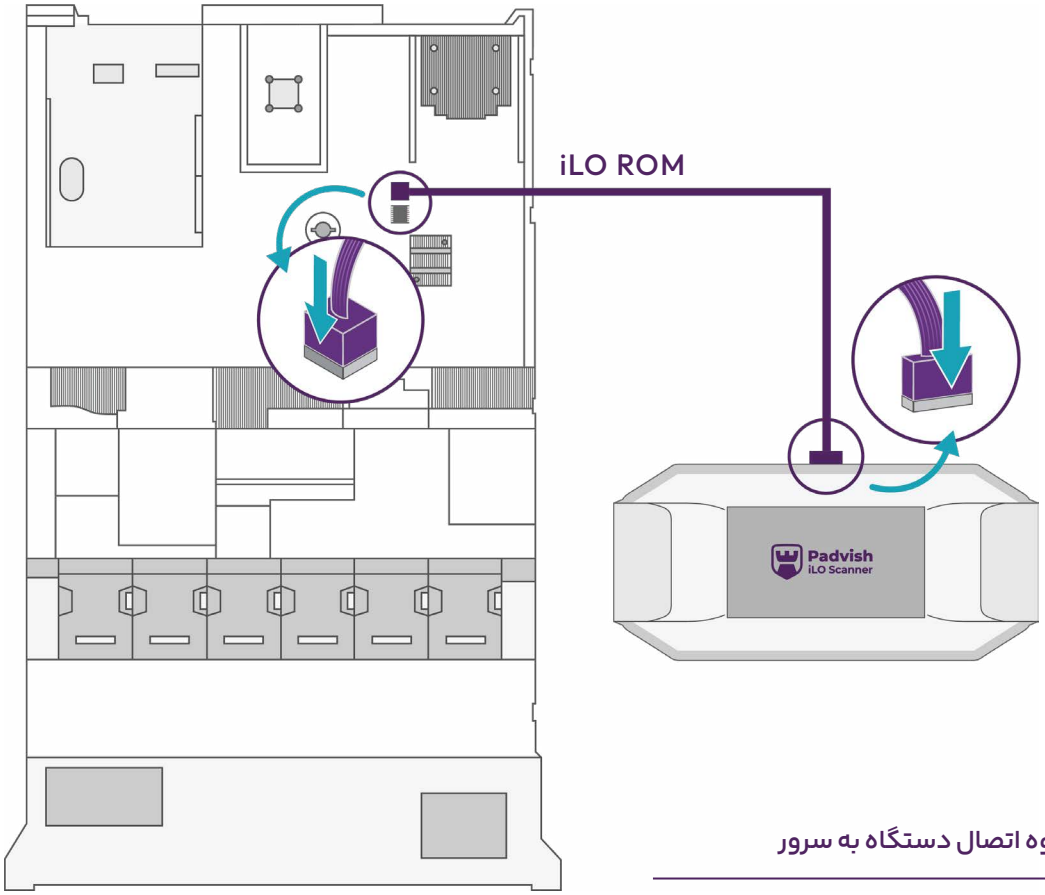
۱ دستگاه Padvish iLO Scanner راهکاری تخصصی برای اعتبارسنجی سفت‌افزار iLO و کشف و پاک‌سازی انواع تهدیدات احتمالی روی این سفت‌افزار است.

۲ این دستگاه به صورت پرتابل و بدون نیاز به اتصال دائم به جریان برق، با بهره‌گیری از یک گیره نوآورانه، به صورت مستقیم به تراشه حاوی سفت‌افزار iLO روی برد سرورهای HP متصل شده و با سرعت و دقت بالا، این سفت‌افزار را پایش می‌کند.

۳ پس از اتمام عملیات پایش و پردازش داده‌ها، دستگاه به سرعت گزارش وضعیت اصالت و به‌روزبودن سفت‌افزار را ارائه می‌دهد.

۴ در صورت وجود آلودگی احتمالی در سفت‌افزار، گزینه به‌روزرسانی محتوای سفت‌افزار به کاربر ارائه می‌شود.

۵ در این شرایط، دستگاه با حداکثر دقت و ایمنی، محتوای سفت‌افزار را با آخرین نسخه سفت‌افزار معتبر ارائه شده توسط شرکت سازنده بازنویسی می‌کند



نحوه اتصال دستگاه به سرور

موارد استفاده و کاربردهای فنی

وجه تمایز و مزیت رقابتی دستگاه

- خواندن محتوای تراشه NOR Flash به صورت On-Board بدون نیاز به جداسازی تراشه از برد
- دارای مدار هوشمند با جبران اثر لودینگ(سلفی و خازنی) مداربار و هشدار اتصال اشتباه گیره به کاربر و قطع جریان جهت جلوگیری اتصال کوتاه در مدار سرور
- پرتابل و بدون نیاز به اتصال دستگاه به رایانه یا جریان برق مستمر
- دارای باتری با ظرفیت ۴۰۰۰ میلی آمپرساعت با قابلیت پایش و پروگرام بیش از ۳۰ دستگاه در هر بار شارژ کامل
- پشتیبانی از کارت حافظه جانبی جهت ذخیره سازی گزارش پایش سفت افزار

ارزش‌های پیشنهادی منحصر به فرد

شناسایی و رفع تهدیدات پیش از ایجاد خسارت

پرتابل و بدون نیاز به اتصال دستگاه به رایانه یا جریان برق مستمر

اعتبارسنجی اصالت و تضمین سلامت سفت‌افزار

بررسی اصالت سفت‌افزار و ارائه گزارش

کاهش زمان و هزینه پاسخ به حادثه

پاک‌سازی بدافزارهای احتمالی از محتوای سفت‌افزار بلافاصله پس از کشف

افزایش اطمینان برای ذی‌نفعان

به‌روزرسانی سفت‌افزار iLO به آخرین نسخه معتبر منتشر شده توسط شرکت HP در کمترین زمان ممکن

خلاقیت و نوآوری

طراحی گیره منحصر به فرد و بدون مشابه خارجی، با قابلیت اتصال به انواع تراشه‌های ۸ و ۱۶ پایه SMD NOR Flash به‌صورت On-Board با ایمنی بالا بدون آسیب به مدارات جانبی

سهولت کاربری

راه‌اندازی و اجرای عملیات پایش و به‌روزرسانی در کمترین زمان بدون نیاز به تخصص

"شرکت نرم افزاری امن پرداز محصولات و خدمات متنوعی را با نام تجاری پادویش جهت مقابله با طیف گسترده تهدیدات و حملات سایبری در بخش خانگی و سازمانی ارائه می نماید."

www.padvish.com
info@amnpardaz.com

درباره ما