هشدار آسیب‌پذیری			
موضوع	آسیب‌پذیری پشته TCP-IP سامانه‌عامل VxWorks		
شماره هشدار	۱۶	**تاریخ صدور هشدار**	۹ مرداد ۱۳۹۸
تشریح تهدید	اخیرا آسیب‌پذیری‌های متنوعی از نوع سرریز پشته (Stack Overflow)، سرریز حافظه هیپ (Heap Overflow)، سرریز عدد صحیح (Integer Overflow)، شرایط رقابتی (Race Condition) و غیره بر روی مولفه پشته TCP/IP سامانه‌عامل VxWorks کشف شده است که این آسیب‌پذیری‌ها به ترتیب اجازه خواهند یک مهاجم از راه دور بتواند وکتورهای حمله دلخواه بر روی دستگاه‌های دارای سامانه‌عامل آسیب‌پذیر VxWorks اجرا کنند. سامانه‌عامل VxWorks یک سامانه‌عامل بلادرنگ (RTOS) است که توسط شرکت Wind River ایجاد شده است. براساس اطلاعات وب‌سایت Wind River، این سامانه‌عامل روی بیش از دو میلیارد دستگاه قرار دارد. سامانه‌عامل‌های بلادرنگ قطعات نرم‌افزاری ساده با ویژگی‌های کمی هستند که روی تراشه‌هایی با دسترسی محدود به منابع مورد استفاده قرار می‌گیرند. یکی از کاربردهای این تراشه‌ها در دستگاه‌های اینترنت اشیا است که در آن‌ها از این تراشه‌ها تنها برای مدیریت عملیات‌های ورودی/خروجی با پردازش داده کم و بدون نیاز به رابط بصری استفاده می‌شود. شایان ذکر است، از این سامانه‌عامل در تجهیزات نظامی و هوافضایی بسیار با اهمیت استفاده شده است، از همین روی این ۱۱ آسیب‌پذیری بسیار بحرانی ارزیابی می‌شوند. یازده آسیب‌پذیری کشف شده در VxWorks در پشته شبکه TCP/IP وجود دارد که یک مولفه در سامانه‌عامل VxWorks است که قابلیت دستگاه برای اتصال به اینترنت یا سایر دستگاه‌ها در شبکه محلی را مدیریت می‌کند. شش مورد از آسیب‌پذیری‌ها بحرانی هستند و منجر به اجرای کد از راه دور می‌شوند که شناسه آنها در زیر آورده شده است: 1. CVE-2019-12256 2. CVE-2019-12255 3. CVE-2019-12260 4. CVE-2019-12261 5. CVE-2019-12263 6. CVE-2019-12257 پنج آسیب‌پذیری دیگر دارای حساسیت کمتری هستند و منجر به ایجاد وضعیت منع سرویس‌دهی، خطاهای منطقی و افشا اطلاعات می‌شوند که شناسه آن ها در زیر آورده شده است: 1. CVE-2019-12258 2. CVE-2019-12262 3. CVE-2019-12264 4. CVE-2019-12259 5. CVE-2019-12265 این آسیب‌پذیری‌ها تمامی نسخه‌های VxWorks RTOS از ۶.۵ به بعد را تحت تاثیر قرار می‌دهند. برخی از این آسیب‌پذیری‌ها قابل بهره‌برداری از طریق اینترنت هستند اما برای سوء استفاده از برخی دیگر نیاز به دسترسی شبکه برای مهاجم وجود دارد. نسخه‌های زیر VxWorks که از پشته شبکه IPnet استفاده می‌کند، تحت تاثیر این آسیب‌پذیری‌ها قرار گرفته‌اند: 1. VxWorks 7 (SR540 and SR610) 2. VxWorks 6.5-6.9 3. Versions of VxWorks using the Interpeak standalone network stack		
راه‌حل کاهش تهدید	برخی از آسیب‌پذیری‌ها در بعضی از دستگاه‌ها اهمیت بیشتری دارند. برای مثال در صورت نفوذ به یک دستگاه مسیریاب یا دیوارآتش که VxWorks را اجرا می‌کند، دسترسی به تمامی دستگاه‌های شبکه خصوصی آن دستگاه فراهم می‌شود اما این		

	آسیب‌پذیری در یک کنترلر صنعتی که به اینترنت متصل نباشد خطر کمتری دارد و شانس کمی برای مهاجم برای سوء استفاده از نقص امنیتی وجود دارد. وصله‌های مربوط به این آسیب‌پذیری‌ها در تاریخ ۱۹ جولایمنتشر شده‌اند و نسخه آخر VxWorks7 (SR620) تحت تاثیر آسیب‌پذیری‌ها قرار ندارد.		
شناسه آسیب‌پذیری	CVE-2019-12256 CVE-2019-12257 CVE-2019-12255 CVE-2019-12260 CVE-2019-12261 CVE-2019-12263 CVE-2019-12258 CVE-2019-12259 CVE-2019-12262 CVE-2019-12264 CVE-2019-12265	**شدت آسیب‌پذیری**	میانگین سطح هشدار این گزارش ۹ است.
منابع	https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/		