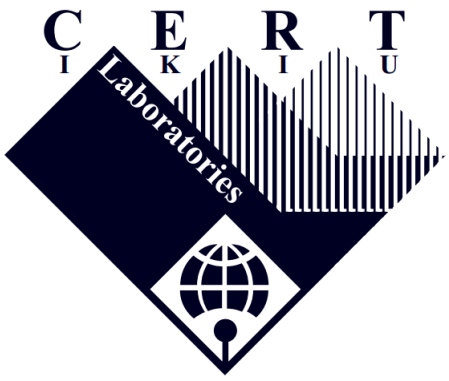


**آزمایشگاه تخصصی آپا، قزوین**

**دانشگاه بین المللی امام خمینی (ره)**

# هفته نامه تحلیلی رویدادهای امنیتی

## شنبه بیست و سوم شهریور ماه ۱۳۹۸

نسخه ۱,۰,۰

بنام خداوند بخشنده و مهربان

## یادداشت سردبیر

عدم تخریب اشیاء،[1] پیوندها و یا سایر عناصر یک برنامه کامپیوتری پس از پایان استفاده آن توسط کاربران می‌تواند بسیار خطرناک باشد. برخی برنامه‌نویس‌ها پس از فرآیند احراز هویت[2] به کمک پیوندها یا اشیاء قابلیت‌های اجرایی مهمی را در اختیار کاربران خود می‌گذارند. مواردی که عدم تخریب آن‌ها پس از پایان استفاده می‌تواند راهی را برای سوءاستفاده مهاجمان سایبری و تلاش برای نفوذ فراهم سازد. موضوعی که دقیقا در هفته گذشته برای خدمات‌رسان‌های دارای مادربرد سوپر میکرو[3] اتفاق افتاده است. به عبارت دیگر در ابزار مدیریتی این مادربردها نوعی پیوندهای دسترسی تولید شده که پس از پایان استفاده حذف نشده است. بر این اساس مهاجمان سایبری می‌توانند با سوءاستفاده از آن‌ها به خدمات‌رسان‌های تولید این شرکت نفوذ کرده و به شنود یا سرقت اطلاعات بپردازند.

علت اصلی یکی دیگر از خبرهای هفته گذشته نیز ضعف در مدیریت اشیاء برنامه‌نویسی است. در این خبر توسعه‌دهندگان سیستم‌عامل اندروید بررسی صحت وجود یک شی را قبل از انجام عملیات بر روی آن فراموش کرده‌اند. بنابر اعلام محققان همین امر می‌تواند منجر به افزایش غیرمجاز سطح مدیریتی در صورت وجود دسترسی فیزیکی به دستگاه قربانی گردد. اما خبر آخر هفته گذشته به کشف یک آسیب‌پذیری بحرانی در سرویس پست الکترونیکی اِگزیم[4] اختصاص دارد. در بهره‌گیری از این آسیب‌پذیری مهاجم هنگام مذاکره اولیه پروتکل تی.ال.اس[5] (برای برقراری ارتباطات امن) با ارسال پیام‌های مخرب به ایجاد اختلال در ارتباطات می‌پردازد. شرایطی که در آن بنا بر اعلام محققان امکان اجرای غیرمجاز برنامه‌ها در سطح دسترسی کاربر روت[6] ممکن است.

محمد پیشدار

[1] In Object-oriented programming, an object is an instance of a Class. Objects are an abstraction. They hold both data, and ways to manipulate the data. The data is usually not visible outside the object.

[2]-Service authentication refers to the identity verification process from the service provider to the user.

[3]-Supermicro, the leader in server technology innovation and green computing, provides customers around the world with application-optimized server, workstation, blade, storage and GPU systems.

[4]-Exim is a mail transfer agent (MTA) used on Unix-like operating systems. Exim is free software distributed under the terms of the GNU General Public License, and it aims to be a general and flexible mailer with extensive facilities for checking incoming e-mail.

[5]-Transport Layer Security is a cryptographic protocol that provide communications security over a computer network.

[6]-in computing, the superuser is a special user account used for system administration. Depending on the operating system (OS), the actual name of this account might be root, administrator, admin or supervisor

## فهرست مطالب

# نمای کلی :

در جدول زیر اطلاعات اخبار هفته گذشته آورده شده است.

| | |
|---|---|
| **امکان نفوذ به خدمات‌رسان‌های ساخت شرکت سوپرمیکرو** | |
| **دستگاه‌های تحت تاثیر** | خدمات‌رسان‌های دارای مادربرد سوپرمیکرو |
| **راه‌های نفوذ** | عبور از فرایند احراز هویت ویژگی یو.اِس.بی[1] مجازی با سوءاستفاده از عدم تخریب پیوندهای برخط در لخت‌افزار[2] مادربردهای سوپرمیکرو |
| **اهداف مهاجمان** | دسترسی به اطلاعات قربانیان از راه دور، شنود اطلاعات |
| **آسیب‌پذیری روز صفر[3] در دستگاه‌های اندروید[4]** | |
| **دستگاه‌های تحت تاثیر** | سیستم‌عامل اندروید |
| **روش نفوذ** | متقاعدسازی قربانی برای نصب و اجرا یک برنامه اندرویدی مخرب |
| **اهداف مهاجمان** | اجرای کدهای دلخواه، کنترل کامل دستگاه اندرویدی |
| **آسیب‌پذیری بحرانی در سرویس پست الکترونیکی اِگزیم[5]** | |
| **دستگاه‌های تحت تاثیر** | خدمات‌رسان‌های سرویس پست الکترونیکی اِگزیم (نسخه ۴٫۸۰ الی ۴٫۹۲٫۱) |
| **روش نفوذ** | ارسال یک نشانگر مخرب نام خدمات‌رسان (اِس.اِن.اِی[6]) هنگام مذاکره اولیه تی.اِل.اِس[7] به خدمات‌رسان قربانی |
| **اهداف مهاجمان** | اجرای کُدهای دلخواه و غیرمجاز از راه دور، ایجاد اختلال در عملکرد تی.اِل.اِس |

[1]-USB is an industry standard that establishes specifications for cables, connectors and protocols for connection, communication and power supply between personal computers and their peripheral devices.
[2]-In computer programming, a software framework is an abstraction in which software providing generic functionality can be selectively changed by additional user-written code, thus providing application-specific software.
[3]-A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software).
[4]-Android is a mobile operating system developed by Google.
[5]-Exim is a mail transfer agent (MTA) used on Unix-like operating systems. Exim is free software distributed under the terms of the GNU General Public License, and it aims to be a general and flexible mailer with extensive facilities for checking incoming e-mail.
[6]-SNI stands for Server Name Indication and is an extension of the TLS protocol. It indicates which hostname is being contacted by the browser at the beginning of the handshake process.
[7]-Transport Layer Security (TLS) is a cryptographic protocol that provide communications security over a computer network.

خبر شماره ۱ تاریخ انتشار : ۹۸/۰۶/۱۷

# امکان نفوذ به خدمات‌رسان‌های ساخت شرکت سوپرمیکرو

خلاصه

بنا بر اعلام محققان، بیش از چهل و هفت هزار خدمات‌رسان دارای مادِربرد سوپرمیکرو تحت تاثیر آسیب‌پذیری جدیدی با عنوان یو.اِس.بی.اِنیور[1] قرار گرفته‌اند. علت اصلی این امر امکان دسترسی اینترنتی به یک مولفه داخلی خدمات‌رسان عنوان شده است. با آسیب‌پذیری مذکور مهاجمان می‌توانند کنترلر مدیریت برد مرکزی (بی.اِم.سی[2]) دستگاه‌های سوپرمیکرو را تحت اختیار خود بگیرند.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=371

مرجع اصلی خبر

Zdnet Website

https://www.zdnet.com/article/over-47000-supermicro-servers-are-exposing-bmc-ports-on-the-internet/

[1]-USBAnywhere

[2]-A baseboard management controller (BMC) is a specialized service processor that monitors the physical state of a computer, network server or other hardware device using sensors and communicating with the system administrator through an independent connection.

خبر شماره ۲ تاریخ انتشار : ۹۸/۰۶/۱۷

# آسیب‌پذیری روز صفر در دستگاه‌های اندروید

خلاصه

اخیرا محققان حوزه امنیت اطلاعات یک آسیب‌پذیری روز صفر را در سیستم‌عامل اندروید کشف کرده‌اند. این نقص مربوط به بخش راه‌انداز[1] رسانه‌ای اندروید بوده و یک مهاجم با بهره‌گیری از آن می‌تواند کنترل کامل دستگاه قربانی را به دست آورد. تا کنون هیچ وصله امنیتی برای این آسیب‌پذیری منتشر نشده است.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=372

مرجع اصلی خبر:

Threatpost Website

https://threatpost.com/android-zero-day-bug-opens-door-to-privilege-escalation-attack-researchers-warn/148014/

[1]-A driver in software provides a programming interface to control and manage specific lower level interface that is often linked to a specific type of hardware, or other low-level service.

خبر شماره ۳ تاریخ انتشار : ۹۸/۰۶/۲۰

# آسیب‌پذیری بحرانی در سرویس پست الکترونیکی اِگزیم

خلاصه

اخیرا محققان حوزه امنیت اطلاعات موفق به کشف یک آسیب‌پذیری اجرای کُد راه دور در خدمات‌رسان‌های نوعی سرویس پست الکترونیکی تحت عنوان اِگزیم (نسخه ۴,۸۰ الی ۴,۹۲,۱) شده‌اند. اِگزیم امروزه بع عنوان یکی از محبوبترین سرویس‌های انتقال پیام در سیستم‌عامل مبتنی بر یونیکس[1] شناخته می‌شود. براساس گزارشات حدود ۶۰ درصد خدمات‌رسان های پست الکترونیکی موجود بر روی اینترنت از این ابزار جهت مسیریابی، ارسال و دریافت پیام استفاده می کنند.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=374

مرجع اصلی خبر:

The Hacker News Website

https://thehackernews.com/2019/09/exim-email-server-vulnerability.html

[1]-Unix is a family of multitasking, multiuser computer operating systems that derive from the original AT&T Unix, development starting in the 1970s at the Bell Labs research center by Ken Thompson, Dennis Ritchie, and others.