Ceritas Vulnerability Alert

# CERITAS ANALYSIS

Hardware and firmware alerts profiled
by a team of Ceritas experts.

## LOOKING BACK AT DEVASTATING HISTORICAL CYBERATTACKS THROUGH THE LENS OF CERITAS.

Even experienced security professionals lack what they need to protect against hardware and firmware threats.

Ceritas helps you harden your infrastructure by auditing IT and OT equipment, exposing known and emerging vulnerabilities, and outlining key mitigation steps required to mitigate threats. Distilled from an in-depth data ecosystem of product, component, manufacturer, and vulnerability data, our simple security preach for 1 million records. rating presents threat information in plain language

The data that Ceritas brings you is easily accessible -- providing proper contextualization for the end-user to quickly understand risk. With Ceritas, you can assess your hardware. quickly identify any flawed components, and make a plan of action.

In this whitepaper, we take a look at 4 past hardware security alerts that could still be affecting your hardware and firmware. Learn more about how Ceritas can help you harden your stack by scheduling a demo today at www.ceritas.ai

### CYBER ATTACKS MEAN BUSINESS LOST

1. Every 40 seconds, a business is victim to cyber attack. (Kaspersky Security Bulletin)
2. 21% of customers will never return post-breach. (Kaspersky Security Bulletin)
3. $401M is the average cost of breach for 1 million records. (IBM Security)

## CASE STUDY: ROWHAMMER ATTACK

### Security Alert

The Rowhammer attack causes “bit flips” by repeatedly accessing data in the dynamic random access memary (DRAM) chip, This creates an electrical charge that can alter information stored in other “memory rows” on a chip. Increased densities of DRAM integrated circuits have led to physically smaller memory cells containing less charge, which results in lower operational noise margins, increased electromagnetic interactions between memory cells, and greater possibility of data loss. Subsequently, cells interfere with each other’s operation which creates disturbance errors and changes in the values of bits stored in affected memory cells.

### Impacts

With increasing demand for devices to became smaller physically without losing their usability, the rows on a RAM chip have become closer together — allowing Rowhammer attacks to become easier and more effective to concuct. Rowhammer attacks can cause unauthorized code to execule and be further exploited by an altacker. It has also been proven thal these attacks can be carried out remotely to a single computer and even over a network. The ease and effectiveness of this style of attack can have devastating consequences for the impacted organization.

### Recommended Response

- With Ceritas, you can easily audit your technology stack to find devices with vulnerable components and faulty design properties.
- Ceritas will also walk you through the appropriate steps to mitigate the potential impact of a Rowhammer attack, such as increasing the refresh rate for all the rows in the memory system, downgrading your motherboards to one that supports Target Row Refresh, and dedicating a counter per row to keep track of row activation.

### Vulnerability Type

The Rowhammer attack is unusual because rather than exploit a logic vulnerability, the attack works to manipulate the physical design properties of the microchip itself - allowing the attacker to gain unauthorized privileges and cause memory corruption. This type of attack affects a range of chips including those produced by SK Hynix, Micron, and Samsung.

## CASE STUDY: MIRAI MALWARE ATTACK

### Security Alert

Mirai malware attack is a type of Distributed Denial of Service (DDoS) attack that exploits vulnerabilities in smart devices containing the ARC embedded processors. Mirai malware is used to create the botnet to launch the attack. Mirai scans the internet for devices that contain the vulnerable ARC processor. Since this processor runs a minimal version of Linux, the username and password is typically sel as a default login, In the first reported incident attackers were armed with lists of default login information, and used Mirai to infect hundreds of thousands of devices, ranging from network routers to printers, with no detection. Since then, the source code for Mirai malware has been posted in public forums and, therefore, has continued to mutate. It has continued to be used to attack IoT devices with default logins as recently as 2020.

### Impacts

In 2016 three websites reported having been the victim of this attack type, which caused large amounts of fake traffic to slow and interrupt access to the websites. This type of attack not only disrupts legitimate traffic to websites, but also has the potential to shut down websites - leading to larger and costlier business disruptions. For example, in the same year as the initial reported attacks, multiple waves of these attacks struck a major DNS provider, Dyn, causing many prominent websites such as GitHub, Twitter, and Netflix to become unavailable.

### Recommended Response

- When using Ceritas you’ll be notified of any IoT devices that could contain the ARC Embedded Processors.
- Ceritas will also advise on potential mitigation tactics such as using a VLAN in the workplace and restricting access of IoT devices only to those with internal users who have been authenticated by the IT Department.

### Vulnerability Type

The vulnerability, first identified and reported in September 2016, exists in smart devices containing the ARC embedded processor and can be exploited remotely by unsophisticated attackers. By exploiting default logins, hackers are able to infect devices and execute DDoS attacks.

# Ceritas Vulnerability Alert

## CASE STUDY: STUXNET ATTACK

### Security Alert

Stuxnet is a cyberweapon that is assumed to have been built jointly by the United States and Israel in a collaborative effort known as Operation Olympic Games. Stuxnet was designed to target a weakness in programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery and industrial processes. Sluxnet reportedly compromised an “air-gapped” system of Iranian PLCs thal controlled their uranium enrichment program, causing the fast-spinning centrifuges to tear themselves apart. Initial exploitation was delivered via USB drive and ruined almost one-fifth of Iran’s nuclear centrifuges.

### Impacts

Stuxnet attacks can have devastating impacts to critical infrastructure sectors such as power generation anc distribution, and water and wastewater systems. Not only are critical infrastructure attacks disruptive to critical systems, but also extremely costly due to lasting damage to the impacted systems.

### Recommended Response

- With Ceritas, you’|! be notified of CPU vulnerabilities that could be exploited by this attack type.
- Ceritas will also provide potential mitigation tactics such as network protection mechanisms.

### Vulnerability Type

This type of attack targets SCADA and PLC systems (e.g., assembly lines or power plants) remotely exploiting CPU design weaknesses to cause a denial of service condition or credential disclosure. Identification of this vulnerability was first found in the Siemens SIMATIC S7-1200 CPU Family.

## CASE STUDY: MELTDOWN ATTACK

### Security Alert

Meltdown attacks exploit a feature inherent in the design of many modern CPUs. These attacks allow an unauthorized and rogue process to silently read a|| memory. Meltdown can affect a wide range of systems, including all devices running outdated versions of iOS, Linux, macOS, or Windows, and the allack cannot be detected once it is carried oul. Many servers and cloud services are also impacted, in addition to the majority of smart devices with embedded devices using ARM-based processors (mobile devices, smart TVs, printers and others), and a wide range of networking equipment. Meltdown attacks also have the potential to impact a wider range of computers than presently identified, as the microprocessor families used in these computers have little to no variation

### Impacts

Meltdown attacks can be severely detrimental as they can allow access to encryption keys and passwords, exposing sensitive information to an unauthorized user.

### Recommended Response

- When using Ceritas you’ll be notified of eny devices containing vulnerable processors. Ceritas will also advise on potential mitigation tactics, such as critical KPTI/KAISER patches.
- Additionally, when procuring new products, Ceritas helps you easily identify which models contain the safest microprocessors.

### Vulnerability Type

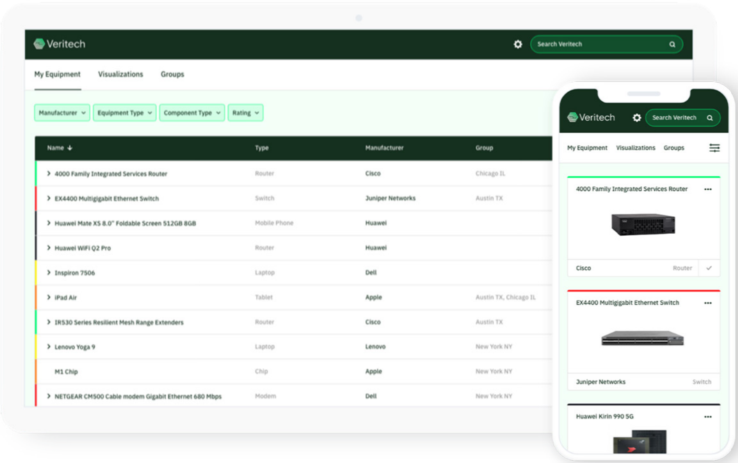
This type of hardware vulnerability impacts intel x86 microprocessors, IBM POWER processors, and some ARM-based microprocessors. The vulnerability is viable on any operating system in which privileged data is mapped into virtual memory for unprivileged processes—which includes many present-day operating systems.

# Ceritas Vulnerability Alert

## HOW CAN CERITAS HELP?

Across verticals, modern organizations are operating complex networks of IT and OT equipment, which can feel impossible to secure. We know you want to keep your company safe, but face a difficult task.

Ceritas combines a proprietary database with AI-powered analytics to identify known and emerging vulnerabilities before they are exploited and irreparably damage your company. With Ceritas, you have the information you need to take action and defend against attack.



| Name ↓ | Type | Manufacturer | Group |
|---|---|---|---|
| 4000 Family Integrated Services Router | Router | Cisco | Chicago IL |
| EX4400 Multigigabit Ethernet Switch | Switch | Juniper Networks | Austin TX |
| Huawei Mate XS 8.0" Foldable Screen 512GB 8GB | Mobile Phone | Huawei | |
| Huawei WiFi Q2 Pro | Router | Huawei | |
| Inspiron 7506 | Laptop | Dell | |
| iPad Air | Tablet | Apple | Austin TX, Chicago IL |
| IR530 Series Resilient Mesh Range Extenders | Router | Cisco | Austin TX |
| Lenovo Yoga 9 | Laptop | Lenovo | New York NY |
| M1 Chip | Chip | Apple | New York NY |
| NETGEAR CM500 Cable modem Gigabit Ethernet 680 Mbps | Modem | Dell | New York NY |

## SIMPLIFYING CYBERSECURITY

Unknown threats in your tech stack may be leaving you vulnerable to a cybersecurity breach

Ceritas distills comprehensive data into one single rating to give you at-a-glance visibility into risks that exist within your IT and OT infrastructure. Our intelligent rating system takes into account the complex nature of hardware and the microelectronics supply chain, but transforms that data into clear action steps, making it easy for you to mitigate vulnerabilities.

**Try Your Free Demo**
of Ceritas

Learn more at **www.ceritas.ai**

## WHAT MAKES CERITAS UNIQUE?

1. Ceritas distills a comprehensive data ecosystem into a simple rating.
2. Clear action steps make it easy for you to mitigate vulnerabilities

## WHY CERITAS?

Our defense-grade platform monitors your current hardware infrastructure and informs future, smart hardware buying decisions.

Ceritas is transforming the defense of hardware. The company is led by a pair of former intelligence officers, trained by the nation's intelligence community to leverage data, analytics, and a global view to identify and anticipate cyber threats.

Ceritas helps you shrink the attack surface and defend against cyber threats.

LEARN MORE AT
**WWW.CERITAS.AI**
Email: katy@ceritas.ai | john@ceritas.ai
Phone: (123) 456-7890