

Neutralizing URGENT/11 on VxWorks Devices with RunSafe Protect

Overview

A U.S. military weapons program needed to protect critical VxWorks-based devices from the widely known URGENT/11 vulnerabilities. By deploying RunSafe Protect, the program eliminated the exploitable ROP gadgets attackers depend on, neutralized URGENT/11 exploits even with the vulnerabilities still present, and strengthened mission-critical systems against future memory-based attacks.

Challenge

In 2019, researchers uncovered URGENT/11, a group of eleven vulnerabilities affecting devices running the widely used VxWorks real-time operating system (RTOS). These flaws, including six critical remote code execution bugs, threatened over two billion embedded devices in industries from healthcare to defense.

Years later, many devices remain unpatched, either because updates are operationally risky, costly, or simply unavailable, leaving essential systems exposed.

Recognizing the risks, a U.S. military weapons program wanted a proven way to take URGENT/11 off the table.



Industry

Aerospace and Defense



Key features

- **Code Hardening:** Randomizes functions at load time, eliminating attacker predictability.
- **Zero-Day Protection:** Stops exploitation attempts, even for unpatched vulnerabilities.
- **URGENT/11 Protection:** Prevents exploitation of six critical memory safety flaws that threaten VxWorks devices.

Solution

RunSafe Security's Protect solution directly targets the type of memory safety vulnerabilities at the heart of URGENT/11. Protect uses a technique called Load-time Function Randomization to defeat attackers who rely on Return-Oriented Programming (ROP), a type of code misuse where adversaries stitch together snippets of legitimate code ("gadgets") to take over systems.

About the Customer

RunSafe worked with the red team of a U.S. military weapons program to validate the effectiveness of Protect in neutralizing URGENT/11 and similar memory safety threats.



About RunSafe

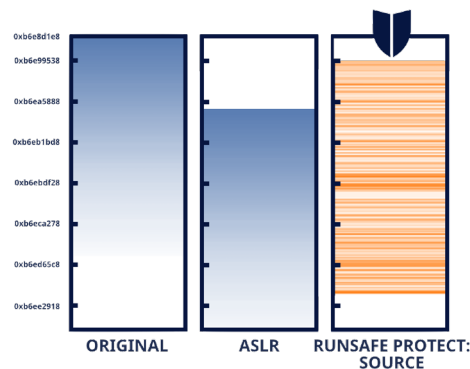
RunSafe Security is the pioneer of a unique cyberhardening technology designed to disrupt attackers and protect vulnerable embedded systems and devices. With the ability to make each device functionally identical but logically unique, RunSafe Security renders threats inert by eliminating attack vectors, significantly reducing vulnerabilities, and denying malware the uniformity required to propagate. Based in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the Industrial Internet of Things (IIoT), critical infrastructure, automotive, and national security industries.



Here's how it works:

- RunSafe Protect randomizes the memory layout of an application every time the software loads.
- With each run, the memory landscape shifts, making it impossible for attackers to predict gadget locations or build a working exploit chain.

The military program's red team tested RunSafe Protect against VxWorks devices still containing the known URGENT/11 flaws. With Protect applied, the red team couldn't find a single usable ROP gadget. Even though the vulnerabilities were still present, the red teamers were unable to exploit the system.



Results

100% Elimination of Exploitable Gadgets

RunSafe cut the system's ROP gadget count from 14,500 to zero.

Neutralized URGENT/11 Exploits—Without Patching

Even with known flaws unpatched, attackers had no viable path to compromise.

Hardened Critical Devices

The weapons program hardened critical embedded devices against one of the most dangerous vulnerability sets of the last decade, ensuring operational continuity and protection against advanced adversaries.

Mission-Critical Resilience

RunSafe Protect is on track to meet DO-178C, aviation's highest safety standard, proving cybersecurity can reinforce mission-critical safety without performance trade-offs.

100% Elimination of
Exploitable Gadgets

Neutralized
URGENT/11

Hardened
Critical Devices

Achieved
Mission-Critical
Resilience