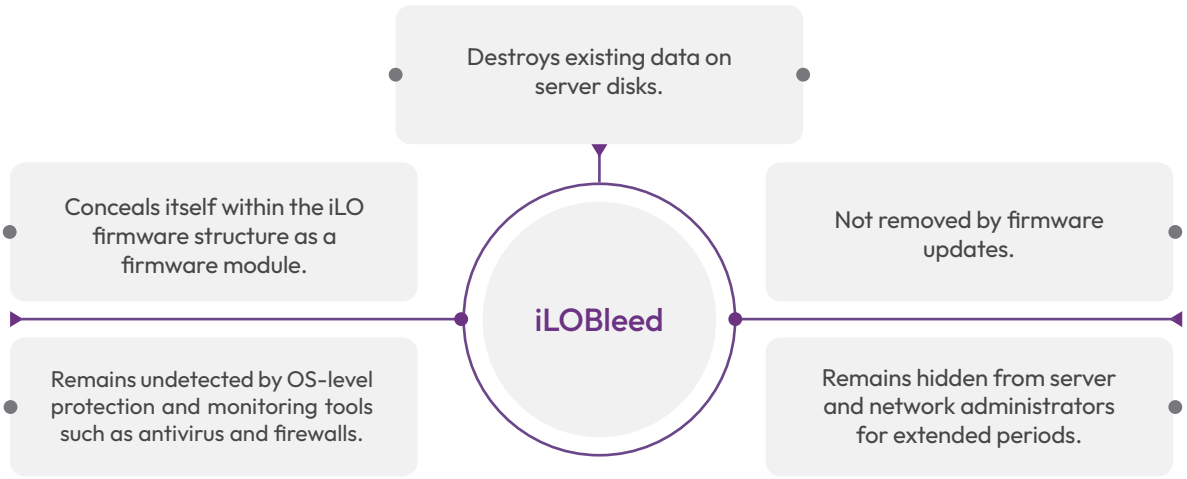
Amnpardaz®
Software Corporation

Padvish
iLO Scanner

Challenges

What Is the iLOBleed Rootkit?

Discovery of the first rootkit in iLO module in HP servers , named Implant.ARM.iLOBleed.a, by the malware analysis team at Amnpardaz Software Corporation.



iLO Module Characteristics

The iLO (Integrated Lights-Out) module in HP servers presents a highly attractive attack surface for intruders and APT groups.

1. This module powers on as soon as the server is connected to a power source.
2. It continues to operate even when the server is shut down (as long as power is not disconnected).
3. This module provides comprehensive access to all server firmware, hardware, software, and the operating system—surpassing any access level available within the OS or hypervisor.
4. The knowledge and tools required to inspect and secure it are not widely available to network administrators.
5. It remains persistent and unchanged even when the operating system is replaced.
6. It provides full administrative access to the server management console for remote power control and OS installation.

Business and Technical Impact of These Challenges

- Imposes financial and reputational damage on the technical and business standing of public and private organizations.
- Sabotage and service disruption through the deletion of all data and services on servers within infrastructure environments.
- Espionage targeting confidential data of sensitive security, military, industrial, and similar centers.
- Could cause irreparable damage to national security and sovereignty if attacks spread.

Solution

Approach

Precise monitoring of iLO firmware using a specialized, reliable tool to detect any infection.

The Padvish iLO Scanner was designed and implemented by Amnpardaz Software Company, leveraging technical expertise and field experience.

Device Design and Implementation Process

- Firmware analysis
- Reverse engineering
- Digital user interface design
- Software development

Padvish iLO Scanner Architecture

- Dedicated clip for direct connection to various 8-pin and 16-pin SMD NOR Flash chips.
- 4.3” capacitive touch user interface.
- STM32F central processor operating at 180 MHz.
- Equipped with two battery modules (7.4 V, 2000 mAh) enabling continuous operation exceeding 6 hours.
- Supports an SD card module for storing reports.

Solution

Key Features and General Capabilities

Direct Monitoring of HP Server iLO Firmware

- Supports HP server generations 8 through 11.
- Creates a copy of the firmware by directly accessing the chip with the server powered off.
- Delivers a report on the authenticity and security status of the installed iLO firmware version using a unique algorithm.

Eliminating Potential Infections and Addressing Security Threats

- Capable of cleaning potential malware present in the iLO firmware, including iLOBleed and others.
- Ability to update the firmware version to the latest valid release provided by HP.

Advanced and Secure

- Accesses the NOR Flash chip content without removing the server from the rack or detaching components from the server board.
- High data transfer speed with compensation for inductive and capacitive loading effects on the target circuit.
- Features an intelligent circuit that compensates for inductive and capacitive loading effects, alerts the user to incorrect clip connection, and cuts power to prevent short circuits on the server board.

Additional Features

1. Identifies the manufacturer, series, and capacity of the NOR Flash chip after clip attachment and before scanning begins.
2. Chip failure warning.
3. Ability to clean infected firmware and update the server to the latest version released by HP.
4. Displays files on the attached SD card (File Explorer).

Technical Specifications

Method of Operation

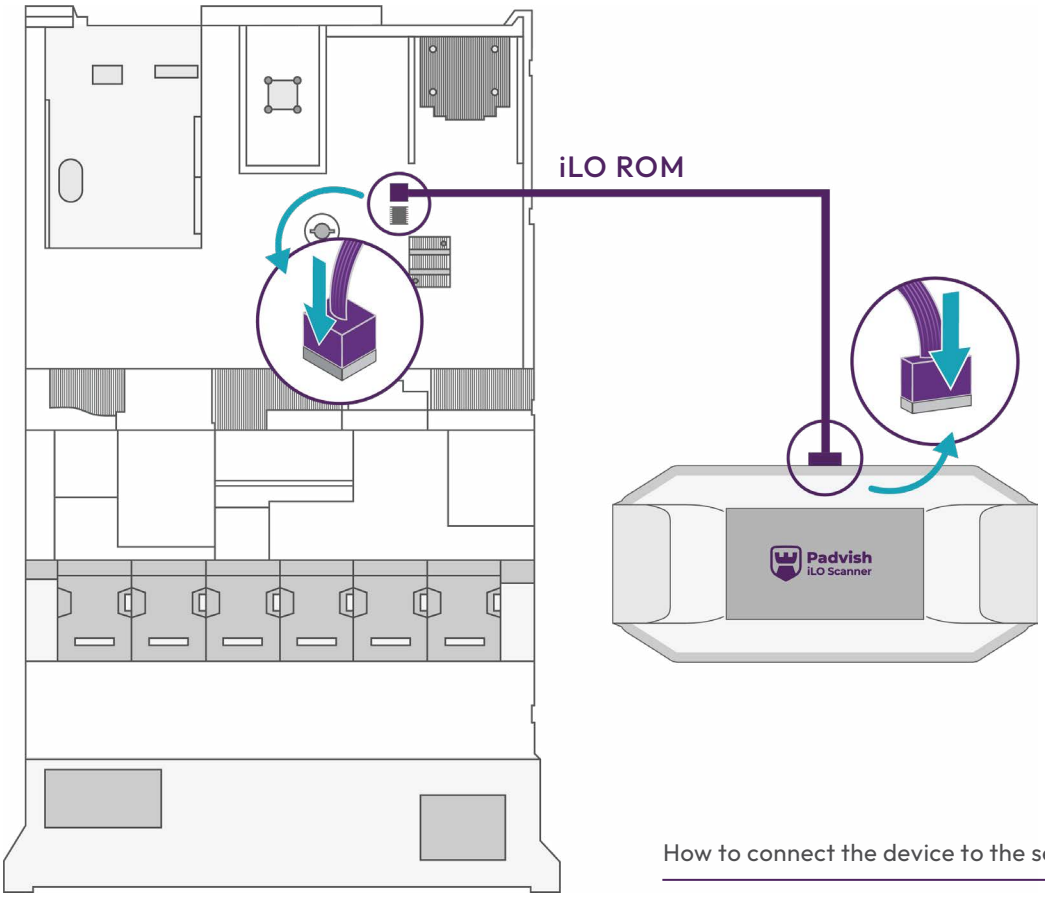
1. The Padvish iLO Scanner is a specialized solution for validating iLO firmware and detecting and cleaning various potential threats within this firmware.

2. Portable and not requiring continuous power, the device uses an innovative clip to connect directly to the chip containing the iLO firmware on HP server boards, scanning the firmware with high speed and accuracy.

3. After scanning and data processing, the device promptly provides a report on the authenticity and up-to-dateness of the firmware.

4. If potential firmware infection is detected, the user is offered the option to update the firmware content.

5. In this case, the device overwrites the firmware content with the latest valid firmware version released by the manufacturer with maximum precision and safety.



How to connect the device to the server

HP G11 Server

Key Advantages and Differentiation

Use Cases and Technical Applications

Differentiator and competitive advantage of the device

1. On-board reading of NOR Flash chip content without requiring chip removal from the board
2. Intelligent circuit compensating for inductive and capacitive loading effects, alerting on incorrect clip connection, and cutting power to prevent short circuits on the server board
3. Portable, no connection to a computer or continuous power required
4. Battery capacity of 4000 mAh, enabling scanning and programming of over 30 devices on a full charge
5. Support for external memory card to store firmware scan reports

Unique Value Propositions

Identify and Resolve Threats Before Damage Occurs

Portable, no connection to a computer or continuous power required.

Authenticity Validation and Firmware Integrity Assurance

Firmware authenticity verification and report generation.

Reduced Incident Response Time and Cost

Immediate cleaning of potential malware from firmware content upon detection.

Increased Confidence

Update iLO firmware to the latest valid version released by HP in the shortest possible time.

Creativity and Innovation

Unique clip design, with no known equivalent, capable of connecting to various 8-pin and 16-pin SMD NOR Flash chips on-board, ensuring high safety and no damage to adjacent circuits.

Ease of Use

Setup and execution of scanning and updating operations in minimal time, without requiring specialized expertise.

“Amnpardaz Software Corporation, operating under the Padvish brand, offers a comprehensive range of cybersecurity solutions tailored to safeguard both home and enterprise environments against evolving cyber threats”

Amnpardaz®
Software Corporation

Padvish®

www.padvish.com
info@amnpardaz.com

Learn More