((Mahdi Keshavarz Research For ➔➔ Sans : Sec275))

((Source: runzero.com website))

((((Research)) ➔➔➔ (Integrated-Lights-Out (iLO))))

What Does Integrated Lights-Out (iLO) Mean?

Integrated Lights-Out (iLO) is a remote server management processor embedded on the system boards of HP ProLiant and Blade servers that allows controlling and monitoring of HP servers from a remote location. HP iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and run servers remotely.

The embedded iLO management card has its own network connection and IP address to which server administrators can connect via Domain Name System (DNS)/Dynamic Host Configuration Protocol (DHCP) or through a separate dedicated management network. iLO provides a remote Web-based console, which can be used to administer the server remotely. The iLO port is an Ethernet port, which can be enabled through the ROM-Based Setup Utility (RBSU).

Bypassing encryption to improve iLO security

HPE's Integrated Lights-Out (iLO) logic is available in many of HPE's server lines, including ProLiant and Gen10 series. Similar to other "lights out" management solutions such as Dell's iDRAC and Supermicro's IPMI boards, iLO supports out-of-band remote management of the servers where it is embedded.

Last year, these security researchers noticed that HPE had begun encrypting the iLO firmware blobs and decided to analyze the new encryption mechanism, with an eye toward surfacing security implications around this new encrypted packaging. Their talk at Black Hat, titled **"HPE iLO5 Firmware Security - Go Home Cryptoprocessor, You're Drunk!"**, digs into their research methods and the vulnerabilities they discovered with iLO. It included a buffer overflow (**CVE-2021-29202**) that can be locally exploited to allow a privileged user of the system OS to execute code as a privileged user on the iLO itself.

In addition to these researchers' findings, a number of other iLO 5 vulnerabilities had been reported to HPE, including XSS and CRLF injection, affecting multiple versions of iLO 5 firmware on HPE servers that include iLO logic. Ultimately, leading HPE to publish a **security bulletin** and a new iLO firmware version: 2.44