



# CVE-2022-23704

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-23704
<b>State</b>	PUBLIC
<b>Assigner</b>	security-alert@hpe.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-05-09 21:15:00 UTC
<b>Updated</b>	2022-05-19 14:50:00 UTC
<b>Description</b>	A potential security vulnerability has been identified in Integrated Lights-Out 4 (iLO 4). The vulnerability could allow remote

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Hp</a>	<a href="#">Integrated Lights-out 4</a>	All	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Apollo 4200 Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant BI420c Gen8 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant BI460c Gen8 Server Blade</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant BI460c Gen9 Server Blade</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant BI465c Gen8 Server Blade</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant BI660c Gen8 Server Blade</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant BI660c Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI120 Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI160 Gen8 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI160 Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI180 Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI20 Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI320e Gen8 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI320e Gen8 V2 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI360e Gen8 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant DI360p Gen8 Server</a>	-	All	All	All

Hardware	Hpe	Proliant DI360 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant DI380e Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant DI380p Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant DI380 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant DI385p Gen8	-	All	All	All
Hardware	Hpe	Proliant DI560 Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant DI560 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant DI580 Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant DI580 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant DI60 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant DI80 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant Ec200a Server	-	All	All	All
Hardware	Hpe	Proliant Microserver Gen8	-	All	All	All
Hardware	Hpe	Proliant MI110 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant MI150 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant MI30 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant MI310e Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant MI310e Gen8 V2 Server	-	All	All	All
Hardware	Hpe	Proliant MI350e Gen8 V2 Server	-	All	All	All
Hardware	Hpe	Proliant MI350p Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant MI350 Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant SI210t Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant SI230s Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant SI250s Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant SI270s Gen8 Server	-	All	All	All
Hardware	Hpe	Proliant SI270s Gen8 Se Server	-	All	All	All
Hardware	Hpe	Proliant SI4540 Gen8 1 Node Server	-	All	All	All
Hardware	Hpe	Proliant Ws460c Gen8 Graphics Server Blade	-	All	All	All
Hardware	Hpe	Proliant Ws460c Gen9 Graphics Server Blade	-	All	All	All
Hardware	Hpe	Proliant XI170r Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant XI190r Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant XI220a Gen8 V2 Server	-	All	All	All
Hardware	Hpe	Proliant XI230a Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant XI250a Gen9 Server	-	All	All	All
Hardware	Hpe	Proliant XI450 Gen9 Server	-	All	All	All

Hardware	<a href="#">Hpe</a>	<a href="#">Proliant XI730f Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant XI740f Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Proliant XI750f Gen9 Server</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Synergy 480 Gen9 Compute Module</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Synergy 620 Gen9 Compute Module</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Synergy 660 Gen9 Compute Module</a>	-	All	All	All
Hardware	<a href="#">Hpe</a>	<a href="#">Synergy 680 Gen9 Compute Module</a>	-	All	All	All

## References

Reference	Source	Link	Tags
Document Display   HPE Support Center	MISC	<a href="https://support.hpe.com">support.hpe.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[730841](#) Hewlett Packard Enterprise (HPE) Integrated Lights-Out 4 (iLO 4) Denial of Service (DoS) (HPESBHF04240)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)