



# CVE-2022-28629

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-28629
<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>	2022-08-12 15:15:00 UTC
<b>Updated</b>	2022-08-16 14:44:00 UTC
<b>Description</b>	A local arbitrary code execution vulnerability was discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Pri

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Hpe	Apollo 2000 Gen10 Plus System	-	All	All	All
Hardware	Hpe	Apollo 4200 Gen10 Server	-	All	All	All
Hardware	Hpe	Apollo 4510 Gen10 System	-	All	All	All
Hardware	Hpe	Apollo 6500 Gen10 Plus System	-	All	All	All
Hardware	Hpe	Apollo 6500 Gen10 System	-	All	All	All
Hardware	Hpe	Apollo N2600 Gen10 Plus	-	All	All	All
Hardware	Hpe	Apollo N2800 Gen10 Plus	-	All	All	All
Hardware	Hpe	Apollo R2600 Gen10	-	All	All	All
Hardware	Hpe	Apollo R2800 Gen10	-	All	All	All
Hardware	Hpe	Edgeline E920d Server Blade	-	All	All	All
Hardware	Hpe	Edgeline E920t Server Blade	-	All	All	All
Hardware	Hpe	Edgeline E920 Server Blade	-	All	All	All
Operating System	Hpe	Integrated Lights-out 5 Firmware	All	All	All	All
Hardware	Hpe	Proliant BI460c Gen10 Server Blade	-	All	All	All
Hardware	Hpe	Proliant DI110 Gen10 Plus Telco Server	-	All	All	All
Hardware	Hpe	Proliant DI120 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant DI160 Gen10 Server	-	All	All	All

Hardware	Hpe	Proliant DI180 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant DI20 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant DI20 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant DI325 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant DI325 Gen10 Plus V2 Server	-	All	All	All
Hardware	Hpe	Proliant DI325 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant DI345 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant DI360 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant DI360 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant DI365 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant DI380 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant DI380 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant DI385 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant DI385 Gen10 Plus V2 Server	-	All	All	All
Hardware	Hpe	Proliant DI385 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant DI560 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant DI580 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant Dx170r Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant Dx190r Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant Dx220n Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant Dx325 Gen10 Plus V2 Server	-	All	All	All
Hardware	Hpe	Proliant Dx360 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant Dx360 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant Dx380 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant Dx380 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant Dx385 Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant Dx385 Gen10 Plus V2 Server	-	All	All	All
Hardware	Hpe	Proliant Dx4200 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant Dx560 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant E910t Server Blade	-	All	All	All
Hardware	Hpe	Proliant E910 Server Blade	-	All	All	All
Hardware	Hpe	Proliant M750 Server Blade	-	All	All	All
Hardware	Hpe	Proliant Microserver Gen10 Plus	-	All	All	All
Hardware	Hpe	Proliant MI110 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant MI30 Gen10 Plus Server	-	All	All	All

Hardware	Hpe	Proliant MI30 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant MI350 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant XI170r Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant XI190r Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant XI220n Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant XI225n Gen10 Plus 1u Node	-	All	All	All
Hardware	Hpe	Proliant XI230k Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant XI270d Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant XI290n Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant XI420 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant XI450 Gen10 Server	-	All	All	All
Hardware	Hpe	Proliant XI645d Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant XI675d Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Proliant XI925g Gen10 Plus Server	-	All	All	All
Hardware	Hpe	Storage File Controller	-	All	All	All
Hardware	Hpe	Storage Performance File Controller	-	All	All	All
Hardware	Hpe	Storeeasy 1460 Storage	-	All	All	All
Hardware	Hpe	Storeeasy 1560 Storage	-	All	All	All
Hardware	Hpe	Storeeasy 1660 Expanded Storage	-	All	All	All
Hardware	Hpe	Storeeasy 1660 Performance Storage	-	All	All	All
Hardware	Hpe	Storeeasy 1660 Storage	-	All	All	All
Hardware	Hpe	Storeeasy 1860 Performance Storage	-	All	All	All
Hardware	Hpe	Storeeasy 1860 Storage	-	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

[730605](#) Hewlett Packard Enterprise (HPE) Integrated Lights-Out 5 (iLO 5) Multiple Vulnerabilities (HPESBHF04333)

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](#)**