Advisory Alert

Alert Number: AAA20220801 **Date:** August 1, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HP	**Critical**	Multiple Vulnerabilities
HP	**High**	Multiple Vulnerabilities

Description

Affected Product	**HP**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-28627, CVE-2022-28628, CVE-2022-28631, CVE-2022-28632)
Description	HP has released a security update addressing multiple critical vulnerabilities that exists in their HPE Integrated Lights-Out 5 (iLO 5) firmware including local arbitrary code execution and Denial of Service (DoS). HP highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers - Prior to 2.71 HPE Apollo 2000, 4200, 6500 Gen10 Plus System, 4200 Gen10 Server, 4510, 6500 Gen10 System, n2600, n2800 Gen10 Plus, r2000 Chassis, r2800 Gen10, r2600 Gen10, r2800 Gen10 - Prior to 2.71 HPE ProLiant XL420 Gen10 Server HPE Edgeline e920, e920d and e920t Server Blade - Prior to 2.71 HPE ProLiant XL925g Gen10 Plus 1U 4-node Configure-to-order Server - Prior to 2.71 HPE Storage File Controller - Prior to 2.71 HPE Storage Performance File Controller - Prior to 2.71 HPE StoreEasy 1460, 1560, 1660, 1860 Storage, 1660 Expanded Storage, 1660, 1860 Performance Storage - Prior to 2.71 HPE ProLiant DL20, DL325, DL345, DL360, DL365, DL380, DL385, DX220n, DX360, DX380, DX385, MicroServer, ML30, XL220n, XL290n, XL645d, XL675d Gen10 Plus server - Prior to 2.71 HPE ProLiant BL460c Gen10 Server Blade - Prior to 2.71 HPE ProLiant DL20, DL120, DL160, DL180, DL325, DL360, DL380, DL385, DL560, DL580, DX170r, DX190r, DX360, DX380, DX385, DX4200, DX560, ML30, ML110, ML350, XL170r, XL190r, XL230k, XL270d, XL450 Gen10 Server - Prior to 2.71 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to 2.71 HPE ProLiant DL325, DL385, DX325 Gen10 Plus v2 server - Prior to 2.71 HPE ProLiant e910, e910t, m750 Server Blade - Prior to 2.71 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to 2.71 HPE ProLiant XL925g Gen10 Plus 1U 4-node Configure-to-order Server - Prior to 2.71
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04333en_us

Affected Product	**HP**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-28626, CVE-2022-28629, CVE-2022-28630, CVE-2022-28633, CVE-2022-28634, CVE-2022-28635, CVE-2022-28636)
Description	HP has released a security update addressing multiple vulnerabilities that exists in their HPE Integrated Lights-Out 5 (iLO 5) firmware including local arbitrary code execution, Denial of Service (DoS), local sensitive information disclosure and local unauthorized data modification. HP highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers - Prior to 2.71 HPE Apollo 2000, 4200, 6500 Gen10 Plus System, 4200 Gen10 Server, 4510, 6500 Gen10 System, n2600, n2800 Gen10 Plus, r2000 Chassis, r2800 Gen10, r2600 Gen10, r2800 Gen10 - Prior to 2.71 HPE ProLiant XL420 Gen10 Server HPE Edgeline e920, e920d and e920t Server Blade - Prior to 2.71 HPE ProLiant XL925g Gen10 Plus 1U 4-node Configure-to-order Server - Prior to 2.71 HPE Storage File Controller - Prior to 2.71 HPE Storage Performance File Controller - Prior to 2.71 HPE StoreEasy 1460, 1560, 1660, 1860 Storage, 1660 Expanded Storage, 1660, 1860 Performance Storage - Prior to 2.71 HPE ProLiant DL20, DL325, DL345, DL360, DL365, DL380, DL385, DX220n, DX360, DX380, DX385, MicroServer, ML30, XL220n, XL290n, XL645d, XL675d Gen10 Plus server - Prior to 2.71 HPE ProLiant BL460c Gen10 Server Blade - Prior to 2.71 HPE ProLiant DL20, DL120, DL160, DL180, DL325, DL360, DL380, DL385, DL560, DL580, DX170r, DX190r, DX360, DX380, DX385, DX4200, DX560, ML30, ML110, ML350, XL170r, XL190r, XL230k, XL270d, XL450 Gen10 Server - Prior to 2.71 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to 2.71 HPE ProLiant DL325, DL385, DX325 Gen10 Plus v2 server - Prior to 2.71 HPE ProLiant e910, e910t, m750 Server Blade - Prior to 2.71 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to 2.71 HPE ProLiant XL925g Gen10 Plus 1U 4-node Configure-to-order Server - Prior to 2.71
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04333en_us

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.