НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220803.15 | 3 августа 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в продуктах HPE

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers: до 2.71 HPE Apollo 2000 Gen10 Plus System: до 2.71 HPE Apollo 4200 Gen10 Plus System: до 2.71 HPE Apollo 4200 Gen10 Server: до 2.71 HPE ProLiant XL420 Gen10 Server: до 2.71 HPE Apollo 4510 Gen10 System: до 2.71 HPE Apollo 6500 Gen10 Plus System: до 2.71 HPE Apollo 6500 Gen10 System: до 2.71 HPE Apollo n2600 Gen10 Plus: до 2.71 HPE Apollo n2800 Gen10 Plus: до 2.71 HPE Apollo r2000 Chassis: до 2.71 HPE Apollo r2800 Gen10: до 2.71 HPE Apollo r2600 Gen10: до 2.71 HPE Edgeline e920 Server Blade: до 2.71 HPE Edgeline e920d Server Blade: до 2.71 HPE Edgeline e920t Server Blade: до 2.71 HPE ProLiant DL20 Gen10 Plus server: до 2.71 HPE ProLiant BL460c Gen10 Server Blade: до 2.71 HPE ProLiant DL20 Gen10 Server: до 2.71 HPE ProLiant DL110 Gen10 Plus Telco server: до 2.71

HPE ProLiant DL120 Gen10 Server: до 2.71
HPE ProLiant DL160 Gen10 Server: до 2.71
HPE ProLiant DL180 Gen10 Server: до 2.71
HPE ProLiant DL325 Gen10 Plus server: до 2.71
HPE ProLiant DL325 Gen10 Plus v2 server: до 2.71
HPE ProLiant DL325 Gen10 Server: до 2.71
HPE ProLiant DL345 Gen10 Plus server: до 2.71
HPE ProLiant DL360 Gen10 Plus server: до 2.71
HPE ProLiant DL360 Gen10 Server: до 2.71
HPE ProLiant DL365 Gen10 Plus server: до 2.71
HPE ProLiant DL380 Gen10 Plus server: до 2.71
HPE ProLiant DL380 Gen10 Server: до 2.71
HPE ProLiant DL385 Gen10 Plus server: до 2.71
HPE ProLiant DL385 Gen10 Plus v2 server: до 2.71
HPE ProLiant DL385 Gen10 Server: до 2.71
HPE ProLiant DL560 Gen10 Server: до 2.71
HPE ProLiant DL580 Gen10 Server: до 2.71
HPE ProLiant DX170r Gen10 server: до 2.71
HPE ProLiant DX190r Gen10 server: до 2.71
HPE ProLiant DX220n Gen10 Plus server: до 2.71
HPE ProLiant DX325 Gen10 Plus v2 server: до 2.71
HPE ProLiant DX360 Gen10 Plus server: до 2.71
HPE ProLiant DX360 Gen10 server: до 2.71
HPE ProLiant DX380 Gen10 Plus server: до 2.71
HPE ProLiant DX380 Gen10 server: до 2.71
HPE ProLiant DX385 Gen10 Plus server: до 2.71
HPE ProLiant DX385 Gen10 Plus v2 server: до 2.71
HPE ProLiant DX4200 Gen10 server: до 2.71
HPE ProLiant DX560 Gen10 server: до 2.71
HPE ProLiant e910 Server Blade: до 2.71
HPE ProLiant e910t Server Blade: до 2.71
HPE ProLiant m750 Server Blade: до 2.71

	HPE ProLiant MicroServer Gen10 Plus: до 2.71 HPE ProLiant ML30 Gen10 Plus server: до 2.71 HPE ProLiant ML30 Gen10 Server: до 2.71 HPE ProLiant ML110 Gen10 Server: до 2.71 HPE ProLiant ML350 Gen10 Server: до 2.71 HPE ProLiant XL170r Gen10 Server: до 2.71 HPE ProLiant XL190r Gen10 Server: до 2.71 HPE ProLiant XL220n Gen10 Plus Server: до 2.71 HPE ProLiant XL225n Gen10 Plus 1U Node: до 2.71 HPE ProLiant XL230k Gen10 Server: до 2.71 HPE ProLiant XL270d Gen10 Server: до 2.71 HPE ProLiant XL290n Gen10 Plus Server: до 2.71 HPE ProLiant XL450 Gen10 Server: до 2.71 HPE ProLiant XL645d Gen10 Plus Server: до 2.71 HPE ProLiant XL675d Gen10 Plus Server: до 2.71 HPE ProLiant XL925g Gen10 Plus 1U 4-node Configure-to-order Server: до 2.71 HPE Storage File Controller: до 2.71 HPE Storage Performance File Controller: до 2.71 HPE StoreEasy 1460 Storage: до 2.71 HPE StoreEasy 1560 Storage: до 2.71 HPE StoreEasy 1660 Expanded Storage: до 2.71 HPE StoreEasy 1660 Performance Storage: до 2.71 HPE StoreEasy 1660 Storage: до 2.71 HPE StoreEasy 1860 Performance Storage: до 2.71 HPE StoreEasy 1860 Storage: до 2.71
Дата выявления	2 августа 2022 г.
Дата обновления	2 августа 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS

MITRE: CVE-2022-28626	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	8.2
MITRE: CVE-2022-28627 CVE-2022-28628	Эксплуатация уязвимости позволяет локальному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.3
MITRE: CVE-2022-28629	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	8.8

MITRE: CVE-2022-28630	Эксплуатация уязвимости позволяет локальному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	8.5
MITRE: CVE-2022-28631 CVE-2022-28632	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.6
MITRE: CVE-2022-28633	Эксплуатация уязвимости позволяет локальному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	8.5

MITRE: CVE-2022-28635 CVE-2022-28636	Эксплуатация уязвимости позволяет локальному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	8.1

Ссылки на источники	http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04333en_us