



Solstice

Sat, 20 Dec 2025 13:11:55 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.0.199

Vulnerabilities by Host

Collapse All | Expand All

192.168.0.199



Severity	CVSS v2.0	VPR Score	EPSS Score	Plugin	Name
CRITICAL	10.0	-	-	138365	Debian DSA-4722-1 : ffmpeg - security update
CRITICAL	10.0	-	-	138646	Debian DSA-4726-1 : nss - security update
CRITICAL	10.0	-	-	161329	Debian DSA-5139-1 : openssl - security update
CRITICAL	10.0	-	-	162549	Debian DSA-5169-1 : openssl - security update
CRITICAL	10.0	-	-	201450	Debian Linux SEoL (10.x)
CRITICAL	10.0	-	-	164472	Debian dla-3082 : exim4 - security update
CRITICAL	10.0	-	-	164946	Debian dla-3103 : lib32z1 - security update
CRITICAL	10.0	-	-	164992	Debian dla-3107 : lemon - security update
CRITICAL	10.0	-	-	166182	Debian dla-3153 : libksba-dev - security update
CRITICAL	10.0	-	-	166779	Debian dla-3175 : idle-python3.7 - security update
CRITICAL	10.0	-	-	167053	Debian dla-3179 : libpixmap-1-0 - security update
CRITICAL	10.0	-	-	169296	Debian dla-3248 : libksba-dev - security update
CRITICAL	10.0	-	-	173849	Debian dla-3381 : ghostscript - security update
CRITICAL	10.0	-	-	174685	Debian dla-3398 : curl - security update
CRITICAL	10.0	-	-	174709	Debian dla-3401 : apache2 - security update
CRITICAL	10.0	-	-	178842	Debian dla-3504 : gir1.2-gst-plugins-base-1.0 - security update
CRITICAL	10.0	-	-	179924	Debian dla-3532 : openssh-client - security update

CRITICAL	10.0	-	-	<a href="#">180518</a>	Debian dla-3555 : libapache2-mod-php7.3 - security update
CRITICAL	10.0	-	-	<a href="#">181562</a>	Debian dla-3570 : libwebp-dev - security update
CRITICAL	10.0	-	-	<a href="#">182416</a>	Debian dla-3598 : libvpx-dev - security update
CRITICAL	10.0	-	-	<a href="#">182430</a>	Debian dla-3599 : exim4 - security update
CRITICAL	10.0	-	-	<a href="#">182942</a>	Debian dla-3614 : idle-python3.7 - security update
CRITICAL	10.0	-	-	<a href="#">58987</a>	PHP Unsupported Version Detection
HIGH	9.4	-	-	<a href="#">169736</a>	Debian dla-3263 : libtasn1-6 - security update
HIGH	9.4	-	-	<a href="#">200647</a>	Debian dla-3830 : libvpx-dev - security update
HIGH	9.3	-	-	<a href="#">149275</a>	Debian DSA-4912-1 : exim4 - security update
HIGH	9.0	-	-	<a href="#">157908</a>	Debian DSA-5071-1 : samba - security update
HIGH	9.0	-	-	<a href="#">158031</a>	Debian DSA-5073-1 : expat - security update
HIGH	9.0	-	-	<a href="#">158761</a>	Debian DSA-5096-1 : linux - security update
HIGH	9.0	-	-	<a href="#">159906</a>	Debian DSA-5122-1 : gzip - security update
HIGH	9.0	-	-	<a href="#">159904</a>	Debian DSA-5123-1 : xz-utils - security update
HIGH	9.0	-	-	<a href="#">164523</a>	Debian dla-3088 : libsnmp-base - security update
HIGH	9.0	-	-	<a href="#">168264</a>	Debian dla-3213 : krb5-admin-server - security update
HIGH	9.0	-	-	<a href="#">176214</a>	Debian dla-3430 : cups-browsed - security update
HIGH	9.0	-	-	<a href="#">177457</a>	Debian dla-3459 : libxpm-dev - security update
HIGH	9.0	-	-	<a href="#">189972</a>	Debian dla-3732 : sudo - security update
HIGH	9.0	-	-	<a href="#">192185</a>	Debian dla-3763 : curl - security update
HIGH	9.0	-	-	<a href="#">194968</a>	Debian dla-3807 : glibc-doc - security update
HIGH	8.5	-	-	<a href="#">214602</a>	Debian DSA-5015-1 : samba - security update
HIGH	8.5	-	-	<a href="#">163433</a>	Debian DSA-5189-1 : gssapi - security update
HIGH	8.3	-	-	<a href="#">197925</a>	Debian dla-3820 : bluetooth - security update
HIGH	8.0	-	-	<a href="#">176347</a>	Debian dla-3432 : idle-python2.7 - security update
HIGH	8.0	-	-	<a href="#">177875</a>	Debian dla-3477 : idle-python3.7 - security update
HIGH	8.0	-	-	<a href="#">201168</a>	Debian dla-3850 : glibc-doc - security update
HIGH	7.9	-	-	<a href="#">148967</a>	Debian DSA-4898-1 : wpa - security update
HIGH	7.8	-	-	<a href="#">157249</a>	Debian DSA-5062-1 : nss - security update
HIGH	7.8	-	-	<a href="#">164081</a>	Debian dla-3070 : gnutls-bin - security update
HIGH	7.8	-	-	<a href="#">164083</a>	Debian dla-3071 : libtirpc-common - security update
HIGH	7.8	-	-	<a href="#">165715</a>	Debian dla-3138 : bind9 - security update
HIGH	7.8	-	-	<a href="#">166091</a>	Debian dla-3151 : squid - security update
HIGH	7.8	-	-	<a href="#">166671</a>	Debian dla-3165 : expat - security update
HIGH	7.8	-	-	<a href="#">170055</a>	Debian dla-3270 : libsnmp-base - security update

HIGH	7.8	-	-	<a href="#">171901</a>	Debian dla-3341 : curl - security update
HIGH	7.8	-	-	<a href="#">175926</a>	Debian dla-3403 : hyperv-daemons - security update
HIGH	7.8	-	-	<a href="#">174964</a>	Debian dla-3405 : libxml2 - security update
HIGH	7.8	-	-	<a href="#">176521</a>	Debian dla-3439 : libwebp-dev - security update
HIGH	7.8	-	-	<a href="#">177254</a>	Debian dla-3454 : ffmpeg - security update
HIGH	7.8	-	-	<a href="#">177636</a>	Debian dla-3472 : libx11-6 - security update
HIGH	7.8	-	-	<a href="#">178479</a>	Debian dla-3498 : bind9 - security update
HIGH	7.8	-	-	<a href="#">179135</a>	Debian dla-3513 : libtiff-dev - security update
HIGH	7.8	-	-	<a href="#">179808</a>	Debian dla-3528 : gir1.2-poppler-0.18 - security update
HIGH	7.8	-	-	<a href="#">181858</a>	Debian dla-3583 : libglib2.0-0 - security update
HIGH	7.8	-	-	<a href="#">182157</a>	Debian dla-3586 : lib32ncurses-dev - security update
HIGH	7.8	-	-	<a href="#">183199</a>	Debian dla-3620 : gir1.2-poppler-0.18 - security update
HIGH	7.8	-	-	<a href="#">189836</a>	Debian dla-3726 : bind9 - security update
HIGH	7.8	-	-	<a href="#">190852</a>	Debian dla-3736 : libunbound-dev - security update
HIGH	7.8	-	-	<a href="#">190998</a>	Debian dla-3740 : gnutls-bin - security update
HIGH	7.8	-	-	<a href="#">191058</a>	Debian dla-3743 : hostapd - security update
HIGH	7.8	-	-	<a href="#">191787</a>	Debian dla-3757 : libnss3 - security update
HIGH	7.8	-	-	<a href="#">191791</a>	Debian dla-3758 : libtiff-dev - security update
HIGH	7.8	-	-	<a href="#">193076</a>	Debian dla-3783 : expat - security update
HIGH	7.8	-	-	<a href="#">194852</a>	Debian dla-3804 : libnghttp2-14 - security update
HIGH	7.8	-	-	<a href="#">195146</a>	Debian dla-3810 : libapache2-mod-php7.3 - security update
HIGH	7.8	-	-	<a href="#">195178</a>	Debian dla-3811 : pypy-idna - security update
HIGH	7.8	-	-	<a href="#">197488</a>	Debian dla-3816 : bind9 - security update
HIGH	7.6	-	-	<a href="#">165477</a>	Debian dla-3119 : expat - security update
HIGH	7.6	-	-	<a href="#">171925</a>	Debian dla-3345 : libapache2-mod-php7.3 - security update
HIGH	7.6	-	-	<a href="#">189756</a>	Debian dla-3724 : python-pil - security update
HIGH	7.5	-	-	<a href="#">135983</a>	Debian DSA-4663-1 : python-reportlab - security update
HIGH	7.5	-	-	<a href="#">140104</a>	Debian DSA-4757-1 : apache2 - security update
HIGH	7.5	-	-	<a href="#">141552</a>	Debian DSA-4774-1 : linux - security update
HIGH	7.5	-	-	<a href="#">142635</a>	Debian DSA-4786-1 : libexif - security update
HIGH	7.5	-	-	<a href="#">149855</a>	Debian DSA-4919-1 : lz4 - security update
HIGH	7.5	-	-	<a href="#">149897</a>	Debian DSA-4920-1 : libx11 - security update
HIGH	7.5	-	-	<a href="#">150705</a>	Debian DSA-4930-1 : libwebp - security update
HIGH	7.5	-	-	<a href="#">151485</a>	Debian DSA-4937-1 : apache2 - security update
HIGH	7.5	-	-	<a href="#">152271</a>	Debian DSA-4951-1 : bluez - security update

HIGH	7.5	-	-	<a href="#">152783</a>	Debian DSA-4963-1 : openssl - security update
HIGH	7.5	-	-	<a href="#">153970</a>	Debian DSA-4982-1 : apache2 - security update
HIGH	7.5	-	-	<a href="#">154263</a>	Debian DSA-4990-1 : ffmpeg - security update
HIGH	7.5	-	-	<a href="#">155769</a>	Debian DSA-5016-1 : nss - security update
HIGH	7.5	-	-	<a href="#">156466</a>	Debian DSA-5035-1 : apache2 - security update
HIGH	7.5	-	-	<a href="#">158270</a>	Debian DSA-5085-1 : expat - security update
HIGH	7.5	-	-	<a href="#">161404</a>	Debian DSA-5140-1 : openldap - security update
HIGH	7.5	-	-	<a href="#">161513</a>	Debian DSA-5147-1 : dpkg - security update
HIGH	7.5	-	-	<a href="#">166426</a>	Debian dla-3152 : glibc-doc - security update
HIGH	7.5	-	-	<a href="#">168183</a>	Debian dla-3204 : vim - security update
HIGH	7.5	-	-	<a href="#">180546</a>	Debian dla-3556 : aom-tools - security update
HIGH	7.5	-	-	<a href="#">182381</a>	Debian dla-3590 : python-renderpm - security update
HIGH	7.5	-	-	<a href="#">192475</a>	Debian dla-3768 : python-pil - security update
HIGH	7.2	-	-	<a href="#">137341</a>	Debian DSA-4699-1 : linux - security update
HIGH	7.2	-	-	<a href="#">139631</a>	Debian DSA-4746-1 : net-snmp - security update
HIGH	7.2	-	-	<a href="#">145471</a>	Debian DSA-4839-1 : sudo - security update
HIGH	7.2	-	-	<a href="#">146052</a>	Debian DSA-4843-1 : linux - security update
HIGH	7.2	-	-	<a href="#">146986</a>	Debian DSA-4867-1 : grub2 - security update
HIGH	7.2	-	-	<a href="#">151890</a>	Debian DSA-4941-1 : linux - security update
HIGH	7.2	-	-	<a href="#">157259</a>	Debian DSA-5059-1 : policykit-1 - security update
HIGH	7.2	-	-	<a href="#">161636</a>	Debian DSA-5149-1 : cups - security update
HIGH	7.2	-	-	<a href="#">162703</a>	Debian DSA-5173-1 : linux - security update
HIGH	7.2	-	-	<a href="#">165623</a>	Debian dla-3131 : hyperv-daemons - security update
HIGH	7.2	-	-	<a href="#">166734</a>	Debian dla-3172 : libxml2 - security update
HIGH	7.2	-	-	<a href="#">167748</a>	Debian dla-3190 : grub-common - security update
HIGH	7.2	-	-	<a href="#">177218</a>	Debian dla-3453 : vim - security update
HIGH	7.2	-	-	<a href="#">181846</a>	Debian dla-3582 : ghostscript - security update
HIGH	7.2	-	-	<a href="#">182369</a>	Debian dla-3588 : vim - security update
HIGH	7.2	-	-	<a href="#">192520</a>	Debian dla-3772 : idle-python3.7 - security update
HIGH	7.2	-	-	<a href="#">197941</a>	Debian dla-3823 : less - security update
HIGH	7.2	-	-	<a href="#">198164</a>	Debian dla-3824 : gir1.2-gst-plugins-base-1.0 - security update
HIGH	7.1	-	-	<a href="#">171626</a>	Debian dla-3321 : gnutls-bin - security update
HIGH	N/A	-	-	<a href="#">146389</a>	Debian DSA-4850-1 : libzstd - security update
HIGH	N/A	-	-	<a href="#">146787</a>	Debian DSA-4859-1 : libzstd - security update
HIGH	N/A	-	-	<a href="#">149020</a>	Debian DSA-4903-1 : gst-plugins-base1.0 - security update

HIGH	N/A	-	-	<a href="#">160402</a>	Debian DSA-5126-1 : ffmpeg - security update
HIGH	N/A	-	-	<a href="#">165217</a>	Debian dla-3112 : bzip2 - security update
HIGH	N/A	-	-	<a href="#">165642</a>	Debian dla-3134 : tzdata - security update
HIGH	N/A	-	-	<a href="#">166562</a>	Debian dla-3161 : tzdata - security update
HIGH	N/A	-	-	<a href="#">166732</a>	Debian dla-3171 : distro-info-data - security update
HIGH	N/A	-	-	<a href="#">167043</a>	Debian dla-3178 : ffmpeg - security update
HIGH	N/A	-	-	<a href="#">214477</a>	Debian dla-3326 : isc-dhcp-client - security update
HIGH	N/A	-	-	<a href="#">171861</a>	Debian dla-3337 : libmariadb-dev - security update
HIGH	N/A	-	-	<a href="#">173399</a>	Debian dla-3366 : tzdata - security update
HIGH	N/A	-	-	<a href="#">174968</a>	Debian dla-3411 : distro-info-data - security update
HIGH	N/A	-	-	<a href="#">175048</a>	Debian dla-3412 : tzdata - security update
HIGH	N/A	-	-	<a href="#">178638</a>	Debian dla-3482 : debian-archive-keyring - security update
HIGH	N/A	-	-	<a href="#">184024</a>	Debian dla-3639 : distro-info-data - security update
HIGH	N/A	-	-	<a href="#">186288</a>	Debian dla-3666 : python3-reportbug - security update
HIGH	N/A	-	-	<a href="#">186663</a>	Debian dla-3684 : tzdata - security update
HIGH	N/A	-	-	<a href="#">189916</a>	Debian dla-3731 : man-db - security update
HIGH	N/A	-	-	<a href="#">193461</a>	Debian dla-3788 : tzdata - security update
HIGH	N/A	-	-	<a href="#">194891</a>	Debian dla-3806 : distro-info-data - security update
MEDIUM	6.9	-	-	<a href="#">136124</a>	Debian DSA-4667-1 : linux - security update
MEDIUM	6.9	-	-	<a href="#">154428</a>	Debian DSA-4993-1 : php7.3 - security update
MEDIUM	6.9	-	-	<a href="#">176664</a>	Debian dla-3445 : cpio - security update
MEDIUM	6.9	-	-	<a href="#">154663</a>	PHP 7.3.x < 7.3.32
MEDIUM	6.8	-	-	<a href="#">138225</a>	Debian DSA-4719-1 : php7.3 - security update
MEDIUM	6.8	-	-	<a href="#">139342</a>	Debian DSA-4741-1 : json-c - security update
MEDIUM	6.8	-	-	<a href="#">139812</a>	Debian DSA-4748-1 : ghostscript - security update
MEDIUM	6.8	-	-	<a href="#">141725</a>	Debian DSA-4776-1 : mariadb-10.3 - security update
MEDIUM	6.8	-	-	<a href="#">146603</a>	Debian DSA-4857-1 : bind9 - security update
MEDIUM	6.8	-	-	<a href="#">147789</a>	Debian DSA-4869-1 : tiff - security update
MEDIUM	6.8	-	-	<a href="#">148305</a>	Debian DSA-4882-1 : openjpeg2 - security update
MEDIUM	6.8	-	-	<a href="#">149229</a>	Debian DSA-4909-1 : bind9 - security update
MEDIUM	6.8	-	-	<a href="#">150905</a>	Debian DSA-4933-1 : nettle - security update
MEDIUM	6.8	-	-	<a href="#">152165</a>	Debian DSA-4947-1 : libsndfile - security update
MEDIUM	6.8	-	-	<a href="#">161689</a>	Debian DSA-5150-1 : rsyslog - security update
MEDIUM	6.8	-	-	<a href="#">164935</a>	Debian dla-3101 : libxslt1-dev - security update
MEDIUM	6.8	-	-	<a href="#">165983</a>	Debian dla-3142 : dbus - security update

MEDIUM	6.8	-	-	<a href="#">167256</a>	Debian dla-3182 : vim - security update
MEDIUM	6.8	-	-	<a href="#">168859</a>	Debian dla-3243 : libapache2-mod-php7.3 - security update
MEDIUM	6.8	-	-	<a href="#">170164</a>	Debian dla-3272 : sudo - security update
MEDIUM	6.8	-	-	<a href="#">171377</a>	Debian dla-3314 : libsdl2-2.0-0 - security update
MEDIUM	6.8	-	-	<a href="#">173763</a>	Debian dla-3377 : libnss-myhostname - security update
MEDIUM	6.8	-	-	<a href="#">176730</a>	Debian dla-3444 : libmariadb-dev - security update
MEDIUM	6.8	-	-	<a href="#">177513</a>	Debian dla-3461 : libfastjson-dev - security update
MEDIUM	6.8	-	-	<a href="#">178958</a>	Debian dla-3508 : hyperv-daemons - security update
MEDIUM	6.8	-	-	<a href="#">181845</a>	Debian dla-3581 : flac - security update
MEDIUM	6.8	-	-	<a href="#">182584</a>	Debian dla-3602 : libx11-6 - security update
MEDIUM	6.8	-	-	<a href="#">182585</a>	Debian dla-3603 : libxpm-dev - security update
MEDIUM	6.8	-	-	<a href="#">182650</a>	Debian dla-3605 : grub-common - security update
MEDIUM	6.8	-	-	<a href="#">183680</a>	Debian dla-3626 : krb5-admin-server - security update
MEDIUM	6.8	-	-	<a href="#">183747</a>	Debian dla-3628 : dbus - security update
MEDIUM	6.8	-	-	<a href="#">186526</a>	Debian dla-3682 : lib32ncurses-dev - security update
MEDIUM	6.8	-	-	<a href="#">200497</a>	Debian dla-3826 : cups - security update
MEDIUM	6.8	-	-	<a href="#">201099</a>	Debian dla-3840 : hyperv-daemons - security update
MEDIUM	6.8	-	-	<a href="#">134944</a>	PHP 7.3.x < 7.3.16 Multiple Vulnerabilities
MEDIUM	6.8	-	-	<a href="#">143449</a>	PHP 7.3.x < 7.3.25 / 7.4.x < 7.4.13 Multiple Vulnerabilities
MEDIUM	6.6	-	-	<a href="#">164676</a>	Debian dla-3096 : ghostscript - security update
MEDIUM	6.5	-	-	<a href="#">138860</a>	Debian DSA-4732-1 : squid - security update
MEDIUM	6.5	-	-	<a href="#">148300</a>	Debian DSA-4883-1 : underscore - security update
MEDIUM	6.5	-	-	<a href="#">158509</a>	Debian DSA-5087-1 : cyrus-sasl2 - security update
MEDIUM	6.5	-	-	<a href="#">183749</a>	Debian dla-3629 : ceph - security update
MEDIUM	6.4	-	-	<a href="#">143439</a>	Debian DSA-4801-1 : brotli - security update
MEDIUM	6.4	-	-	<a href="#">146613</a>	Debian DSA-4856-1 : php7.3 - security update
MEDIUM	6.4	-	-	<a href="#">166429</a>	Debian dla-3157 : bluetooth - security update
MEDIUM	6.4	-	-	<a href="#">171786</a>	Debian dla-3327 : libnss3 - security update
MEDIUM	6.4	-	-	<a href="#">171749</a>	Debian dla-3331 : python-cryptography - security update
MEDIUM	6.4	-	-	<a href="#">171753</a>	Debian dla-3332 : libaprutil1 - security update
MEDIUM	6.4	-	-	<a href="#">172599</a>	Debian dla-3363 : libpcre2-16-0 - security update
MEDIUM	6.4	-	-	<a href="#">182762</a>	Debian dla-3610 : python-urllib3 - security update
MEDIUM	6.4	-	-	<a href="#">187271</a>	Debian dla-3692 : curl - security update
MEDIUM	6.4	-	-	<a href="#">141355</a>	PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Multiple Vulnerabilities
MEDIUM	6.4	-	-	<a href="#">134162</a>	PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities

MEDIUM	6.2	-	-	<a href="#">177890</a>	Debian dla-3476 : cups - security update
MEDIUM	6.2	-	-	<a href="#">182417</a>	Debian dla-3594 : cups - security update
MEDIUM	6.2	-	-	<a href="#">185377</a>	Debian dla-3649 : python-urllib3 - security update
MEDIUM	6.1	-	-	<a href="#">166004</a>	Debian dla-3146 : isc-dhcp-client - security update
MEDIUM	6.1	-	-	<a href="#">189721</a>	Debian dla-3722 : libmariadb-dev - security update
MEDIUM	6.1	-	-	<a href="#">193175</a>	Debian dla-3786 : python-pil - security update
MEDIUM	6.0	-	-	<a href="#">200694</a>	Debian dla-3831 : nano - security update
MEDIUM	5.8	-	-	<a href="#">159229</a>	Debian DSA-5108-1 : tiff - security update
MEDIUM	5.8	-	-	<a href="#">162701</a>	Debian DSA-5174-1 : gnupg2 - security update
MEDIUM	5.8	-	-	<a href="#">165592</a>	Debian dla-3126 : libsndfile1 - security update
MEDIUM	5.8	-	-	<a href="#">166708</a>	Debian dla-3167 : lib32ncurses-dev - security update
MEDIUM	5.8	-	-	<a href="#">181187</a>	Debian dla-3559 : libssh2-1 - security update
MEDIUM	5.8	-	-	<a href="#">186966</a>	Debian dla-3689 : bluetooth - security update
MEDIUM	5.5	-	-	<a href="#">164482</a>	Debian dla-3085 : curl - security update
MEDIUM	5.5	-	-	<a href="#">181444</a>	Debian dla-3563 : ctdb - security update
MEDIUM	5.4	-	-	<a href="#">177421</a>	Debian dla-3456 : python-requests - security update
MEDIUM	5.4	-	-	<a href="#">182933</a>	Debian dla-3613 : curl - security update
MEDIUM	5.4	-	-	<a href="#">186205</a>	Debian dla-3660 : gnutls-bin - security update
MEDIUM	5.4	-	-	<a href="#">187315</a>	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.0	-	-	<a href="#">136123</a>	Debian DSA-4666-1 : openldap - security update
MEDIUM	5.0	-	-	<a href="#">136721</a>	Debian DSA-4689-1 : bind9 - security update
MEDIUM	5.0	-	-	<a href="#">142189</a>	Debian DSA-4782-1 : openldap - security update
MEDIUM	5.0	-	-	<a href="#">143002</a>	Debian DSA-4792-1 : openldap - security update
MEDIUM	5.0	-	-	<a href="#">143194</a>	Debian DSA-4795-1 : krb5 - security update
MEDIUM	5.0	-	-	<a href="#">144691</a>	Debian DSA-4822-1 : p11-kit - security update
MEDIUM	5.0	-	-	<a href="#">146122</a>	Debian DSA-4845-1 : openldap - security update
MEDIUM	5.0	-	-	<a href="#">146599</a>	Debian DSA-4855-1 : openssl - security update
MEDIUM	5.0	-	-	<a href="#">146786</a>	Debian DSA-4860-1 : openldap - security update
MEDIUM	5.0	-	-	<a href="#">148172</a>	Debian DSA-4873-1 : squid - security update
MEDIUM	5.0	-	-	<a href="#">148277</a>	Debian DSA-4881-1 : curl - security update
MEDIUM	5.0	-	-	<a href="#">148314</a>	Debian DSA-4884-1 : ldb - security update
MEDIUM	5.0	-	-	<a href="#">150165</a>	Debian DSA-4924-1 : squid - security update
MEDIUM	5.0	-	-	<a href="#">151423</a>	Debian DSA-4935-1 : php7.3 - security update
MEDIUM	5.0	-	-	<a href="#">152068</a>	Debian DSA-4944-1 : krb5 - security update
MEDIUM	5.0	-	-	<a href="#">154707</a>	Debian DSA-4994-1 : bind9 - security update

MEDIUM	5.0	-	-	<a href="#">159466</a>	Debian DSA-5111-1 : zlib - security update
MEDIUM	5.0	-	-	<a href="#">165449</a>	Debian dla-3120 : gir1.2-poppler-0.18 - security update
MEDIUM	5.0	-	-	<a href="#">170757</a>	Debian dla-3288 : curl - security update
MEDIUM	5.0	-	-	<a href="#">171643</a>	Debian dla-3325 : libssl-dev - security update
MEDIUM	5.0	-	-	<a href="#">172449</a>	Debian dla-3351 : apache2 - security update
MEDIUM	5.0	-	-	<a href="#">176985</a>	Debian dla-3449 : libssl-dev - security update
MEDIUM	5.0	-	-	<a href="#">179900</a>	Debian dla-3530 : libssl-dev - security update
MEDIUM	5.0	-	-	<a href="#">181697</a>	Debian dla-3575 : idle-python2.7 - security update
MEDIUM	5.0	-	-	<a href="#">183195</a>	Debian dla-3621 : libnghttp2-14 - security update
MEDIUM	5.0	-	-	<a href="#">183996</a>	Debian dla-3634 : libnss3 - security update
MEDIUM	5.0	-	-	<a href="#">214479</a>	Debian dla-3708 : exim4 - security update
MEDIUM	5.0	-	-	<a href="#">189095</a>	Debian dla-3709 : squid - security update
MEDIUM	5.0	-	-	<a href="#">197924</a>	Debian dla-3818 : apache2 - security update
MEDIUM	5.0	-	-	<a href="#">200704</a>	Debian dla-3833 : libapache2-mod-php7.3 - security update
MEDIUM	5.0	-	-	<a href="#">140532</a>	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability
MEDIUM	5.0	-	-	<a href="#">136741</a>	PHP 7.2.x < 7.2.31 / 7.3.x < 7.3.18, 7.4.x < 7.4.6 Denial of Service (DoS)
MEDIUM	5.0	-	-	<a href="#">135918</a>	PHP 7.3.x < 7.3.17 Out of Bounds Read Vulnerability
MEDIUM	5.0	-	-	<a href="#">144947</a>	PHP 7.3.x < 7.3.26 / 7.4.x < 7.4.14 / 8.x < 8.0.1 Input Validation Error
MEDIUM	5.0	-	-	<a href="#">146311</a>	PHP 7.3.x < 7.3.27 / 7.4.x < 7.4.15 / 8.x < 8.0.2 DoS
MEDIUM	5.0	-	-	<a href="#">155590</a>	PHP 7.3.x < 7.3.33
MEDIUM	5.0	-	-	<a href="#">142591</a>	PHP < 7.3.24 Multiple Vulnerabilities
MEDIUM	5.0	-	-	<a href="#">152853</a>	PHP < 7.3.28 Email Header Injection
MEDIUM	5.0	-	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	4.9	-	-	<a href="#">151833</a>	Debian DSA-4942-1 : systemd - security update
MEDIUM	4.9	-	-	<a href="#">165206</a>	Debian dla-3110 : libglib2.0-0 - security update
MEDIUM	4.9	-	-	<a href="#">170881</a>	Debian dla-3297 : libtiff-dev - security update
MEDIUM	4.9	-	-	<a href="#">171785</a>	Debian dla-3333 : libtiff-dev - security update
MEDIUM	4.9	-	-	<a href="#">176635</a>	Debian dla-3440 : cups - security update
MEDIUM	4.9	-	-	<a href="#">179419</a>	Debian dla-3519 : ghostscript - security update
MEDIUM	4.9	-	-	<a href="#">181835</a>	Debian dla-3579 : elfutils - security update
MEDIUM	4.9	-	-	<a href="#">191776</a>	Debian dla-3755 : tar - security update
MEDIUM	4.9	-	-	<a href="#">192521</a>	Debian dla-3771 : idle-python2.7 - security update
MEDIUM	4.6	-	-	<a href="#">139099</a>	Debian DSA-4735-1 : grub2 - security update
MEDIUM	4.6	-	-	<a href="#">144043</a>	Debian DSA-4808-1 : apt - security update
MEDIUM	4.6	-	-	<a href="#">175045</a>	Debian dla-3414 : avahi-autoipd - security update



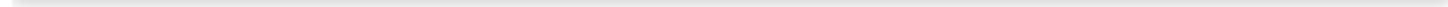
MEDIUM	4.6	-	-	<a href="#">177792</a>	Debian dla-3474 : libnss-myhostname - security update
MEDIUM	4.6	-	-	<a href="#">179933</a>	Debian dla-3524 : hyperv-daemons - security update
MEDIUM	4.4	-	-	<a href="#">214473</a>	Debian dla-3694 : openssh-client - security update
MEDIUM	4.3	-	-	<a href="#">136591</a>	Debian DSA-4685-1 : apt - security update
MEDIUM	4.3	-	-	<a href="#">141841</a>	Debian DSA-4777-1 : freetype - security update
MEDIUM	4.3	-	-	<a href="#">143593</a>	Debian DSA-4807-1 : openssl - security update
MEDIUM	4.3	-	-	<a href="#">148170</a>	Debian DSA-4875-1 : openssl - security update
MEDIUM	4.3	-	-	<a href="#">154750</a>	Debian DSA-4997-1 : tiff - security update
MEDIUM	4.3	-	-	<a href="#">155709</a>	Debian DSA-5014-1 : icu - security update
MEDIUM	4.3	-	-	<a href="#">156563</a>	Debian DSA-5038-1 : ghostscript - security update
MEDIUM	4.3	-	-	<a href="#">158979</a>	Debian DSA-5103-1 : openssl - security update
MEDIUM	4.3	-	-	<a href="#">161434</a>	Debian DSA-5142-1 : libxml2 - security update
MEDIUM	4.3	-	-	<a href="#">162562</a>	Debian DSA-5171-1 : squid - security update
MEDIUM	4.3	-	-	<a href="#">165327</a>	Debian dla-3118 : unzip - security update
MEDIUM	4.3	-	-	<a href="#">170240</a>	Debian dla-3278 : libtiff-dev - security update
MEDIUM	4.3	-	-	<a href="#">175805</a>	Debian dla-3424 : pypy-ipaddress - security update
MEDIUM	4.3	-	-	<a href="#">180269</a>	Debian dla-3548 : libqpdf-dev - security update
MEDIUM	4.3	-	-	<a href="#">189094</a>	Debian dla-3710 : hyperv-daemons - security update
MEDIUM	4.3	-	-	<a href="#">193481</a>	Debian dla-3781 : libgd-dev - security update
MEDIUM	4.0	-	-	<a href="#">139929</a>	Debian DSA-4751-1 : squid - security update
MEDIUM	4.0	-	-	<a href="#">139930</a>	Debian DSA-4752-1 : bind9 - security update
MEDIUM	4.0	-	-	<a href="#">159109</a>	Debian DSA-5105-1 : bind9 - security update
MEDIUM	4.0	-	-	<a href="#">177451</a>	Debian dla-3458 : libapache2-mod-php7.3 - security update
MEDIUM	4.0	-	-	<a href="#">193744</a>	Debian dla-3792 : ctdb - security update
MEDIUM	N/A	-	-	<a href="#">165219</a>	Debian dla-3114 : libmariadb-dev - security update
LOW	3.3	-	-	<a href="#">139569</a>	PHP 7.3.x < 7.3.21 Use-After-Free Vulnerability
LOW	2.1	-	-	<a href="#">144041</a>	Debian DSA-4809-1 : python-apt - security update
LOW	2.1	-	-	<a href="#">164674</a>	Debian dla-3094 : flac - security update
LOW	2.1	-	-	<a href="#">214466</a>	Debian dla-3371 : libunbound-dev - security update
LOW	2.1	-	-	<a href="#">177492</a>	Debian dla-3466 : avahi-autoipd - security update
LOW	2.1	-	-	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
LOW	1.9	-	-	<a href="#">167055</a>	Debian dla-3181 : sudo - security update
LOW	1.9	-	-	<a href="#">169294</a>	Debian dla-3245 : hyperv-daemons - security update
LOW	1.7	-	-	<a href="#">196946</a>	Debian dla-3814 : libglib2.0-0 - security update
LOW	1.2	-	-	<a href="#">192962</a>	Debian dla-3782 : bsduutils - security update

INFO	N/A	-	-	<a href="#">141394</a>	Apache HTTP Server Installed (Linux)
INFO	N/A	-	-	<a href="#">142640</a>	Apache HTTP Server Site Enumeration
INFO	N/A	-	-	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	-	-	<a href="#">34098</a>	BIOS Info (SSH)
INFO	N/A	-	-	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	<a href="#">39521</a>	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	-	<a href="#">182774</a>	Curl Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">55472</a>	Device Hostname
INFO	N/A	-	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	-	<a href="#">25203</a>	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	-	<a href="#">25202</a>	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	-	<a href="#">33276</a>	Enumerate MAC Addresses via SSH
INFO	N/A	-	-	<a href="#">170170</a>	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	-	<a href="#">179200</a>	Enumerate the Network Routing configuration via SSH
INFO	N/A	-	-	<a href="#">168980</a>	Enumerate the PATH Variables
INFO	N/A	-	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	-	-	<a href="#">10092</a>	FTP Server Detection
INFO	N/A	-	-	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	<a href="#">171410</a>	IP Assignment Method Detection
INFO	N/A	-	-	<a href="#">151883</a>	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	-	-	<a href="#">157358</a>	Linux Mounted Devices
INFO	N/A	-	-	<a href="#">193143</a>	Linux Time Zone Information
INFO	N/A	-	-	<a href="#">95928</a>	Linux User List Enumeration
INFO	N/A	-	-	<a href="#">130626</a>	MariaDB Client/Server Installed (Linux)
INFO	N/A	-	-	<a href="#">17651</a>	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	-	<a href="#">10859</a>	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	<a href="#">60119</a>	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	-	-	<a href="#">10395</a>	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	-	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)

INFO	N/A	-	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">64582</a>	Netstat Connection Information
INFO	N/A	-	-	<a href="#">14272</a>	Netstat Portscanner (SSH)
INFO	N/A	-	-	<a href="#">209654</a>	OS Fingerprints Detected
INFO	N/A	-	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	-	<a href="#">97993</a>	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	-	<a href="#">117887</a>	OS Security Patch Assessment Available
INFO	N/A	-	-	<a href="#">181418</a>	OpenSSH Detection
INFO	N/A	-	-	<a href="#">168007</a>	OpenSSL Installed (Linux)
INFO	N/A	-	-	<a href="#">216936</a>	PHP Scripting Language Installed (Unix)
INFO	N/A	-	-	<a href="#">48243</a>	PHP Version Detection
INFO	N/A	-	-	<a href="#">179139</a>	Package Manager Packages Report (nix)
INFO	N/A	-	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	-	<a href="#">10263</a>	SMTP Server Detection
INFO	N/A	-	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	-	<a href="#">102094</a>	SSH Commands Require Privilege Escalation
INFO	N/A	-	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	-	<a href="#">90707</a>	SSH SCP Protocol Detection
INFO	N/A	-	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	-	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	-	-	<a href="#">104887</a>	Samba Version
INFO	N/A	-	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	-	<a href="#">11153</a>	Service Detection (HELP Request)
INFO	N/A	-	-	<a href="#">22869</a>	Software Enumeration (SSH)
INFO	N/A	-	-	<a href="#">49692</a>	Squid Proxy Version Detection
INFO	N/A	-	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	-	<a href="#">110385</a>	Target Credential Issues by Authentication Protocol - Insufficient Privilege
INFO	N/A	-	-	<a href="#">141118</a>	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	-	<a href="#">56468</a>	Time of Last System Startup
INFO	N/A	-	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">192709</a>	Tukaani XZ Utils Installed (Linux / Unix)

INFO	N/A	-	-	<a href="#">110483</a>	Unix / Linux Running Processes Information
INFO	N/A	-	-	<a href="#">152742</a>	Unix Software Discovery Commands Available
INFO	N/A	-	-	<a href="#">189731</a>	Vim Installed (Linux)
INFO	N/A	-	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	<a href="#">182848</a>	libcurl Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">66717</a>	mDNS Detection (Local Network)

Hide



© 2025 Tenable™, Inc. All rights reserved.