Progress®
Kemp® LoadMaster®

# LoadMaster Vulnerabilities

**Generated on: 10 March 2025**

# Copyright

**Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend:** Product Documentation Copyright Notice & Trademarks | Progress

# Table of Contents

**Chapter 1: Vulnerabilities . . . . . 4**

**Chapter 2: CVE-2022-0778: Upgrade Guidance. . . . . 30**

# 1

# Vulnerabilities

The following table lists the security vulnerabilities that the LoadMaster Support Team gets the most queries about. If you have a question about a vulnerability that is not listed below and whether it applies to the LoadMaster Operating System (LMOS) or not, contact Progress Kemp Support.

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2024-31309<br>CVE-2024-30255<br>CVE-2024-28182<br>CVE-2024-27983<br>CVE-2024-27919<br>CVE-2024-27316<br>CVE-2024-27268<br>CVE-2024-2758<br>CVE-2024-2653<br>CVE-2023-45288 | kernel | N/A | Theoretically vulnerable. This is the HTTP/2 CONTINUATION flood vulnerability.<br><br>While there have been no known exploits of this vulnerability on LoadMaster and while LoadMaster does not use any of the vulnerable software listed in the CVEs at left (and in the security notice), it has not yet been proven that LoadMaster is not vulnerable. |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2024-25638 | dnsjava | N/A | Not vulnerable. LoadMaster does not support the dnsjava implementation of DNS. |
| CVE-2024-21626 | N/A | N/A | Not vulnerable. LoadMaster does not support the 'runc' Linux container Command Line Interface (CLI) tool. |
| CVE-2024-7591 | Application Programming Interface (API)/User Interface (UI) | Add-on | Vulnerable. An add-on package is available that closes this vulnerability. Refer to this Knowledge Base article for more information. |
| CVE-2024-8755 | API/UI | Add-on | Vulnerable. An add-on package is available that closes this vulnerability. Refer to this Knowledge Base article for more information. |
| CVE-2024-6658 | API/UI | 7.2.60.1<br>7.2.54.12<br>7.1.35.12 | Vulnerable. A fix for this issue will be made available on the dates shown in this Knowledge Base article. |
| CVE-2024-6387 | openssh | N/A | Not vulnerable in non-FIPS mode: the version of OpenSSH used by LoadMaster in non-FIPS mode is not vulnerable to this exploit.<br><br>Vulnerable in FIPS mode: FIPS mode is vulnerable to this issue, which will be addressed in a future release. To mitigate this issue, ensure that the system management interface is located on a restricted, secure network |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | that can only be accessed by trusted personnel, as described in our system hardening guidelines. |
| CVE-2024-3596 | RADIUS | N/A | Vulnerable. To mitigate this vulnerability it is recommend that all non-accounting-related RADIUS communications between LoadMaster and the RADIUS server be confined to a network that is accessible only by trusted administrative personnel, that no proxies are used between the LoadMaster and the RADIUS server, and that RADIUS client configurations are updated as described in this security notice from the freeRADIUS project. |
| CVE-2024-3544<br>CVE-2024-3543 | API | 7.2.59.4<br>7.2.54.10<br>7.2.48.12 | Vulnerable. Using a specially crafted API call, unauthorized users can gain privileged access to LoadMaster and then use that access to reverse engineer passwords. Refer to this Knowledge Base article for more information. |
| CVE-2024-3094 | N/A | N/A | Not vulnerable. LoadMaster does not support the XZ Utils data compression library. |
| CVE-2024-2511 | openssl | TBD | Vulnerable only when operating in non-FIPS mode. Unbounded memory growth is partially mitigated by the automatic restarting of system processes. This low severity |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | exploit will be closed in a future release. |
| CVE-2024-2449 | API/UI | 7.2.59.3<br>7.2.54.9<br>7.2.48.11<br>7.1.35.11 | Vulnerable. It is possible for a malicious actor, who has prior knowledge of the IP address or hostname of a specific LoadMaster, to direct a currently logged-in administrative user to another third-party site. In such a scenario, the admin user can send HTTP requests to the UI to execute actions on LoadMaster. This vulnerability has been closed by enhancing the validation performed when CSRF checks are performed. Refer to this Knowledge Base article for more information. |
| CVE-2024-2448 | API/UI | 7.2.59.3<br>7.2.54.9<br>7.2.48.11<br>7.1.35.11 | Vulnerable. A logged-in UI user with any permission settings may be able to inject commands into the UI using a shell command that will execute the command in the context of that page and only for that user. This vulnerability has been closed by enhancing the validation performed by the UI. Refer to this Knowledge Base article for more information. |
| CVE-2024-2201 | N/A | N/A | Theoretically vulnerable. This is a CPU vulnerability on Intel platforms that is related to two earlier CVEs: CVE-2022-0001 and CVE-2022-0002. All LoadMaster hardware models are built on CPUs that are vulnerable to this exploit. Any virtual LoadMaster running on |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | an Intel-based hypervisor system may also be theoretically vulnerable. LoadMaster, however, is a purpose-built appliance that does not provide a general purpose Linux shell that could be leveraged to exploit the vulnerability. |
| CVE-2024-1212 | API | 7.2.59.2<br>7.2.54.8<br>7.2.48.10 | Vulnerable. Unauthenticated, remote attackers who have access to the network and port on which API access is configured can issue a carefully crafted API command that will allow arbitrary system commands to be executed without authentication. This critical security issue can be closed by installing one of the patches listed at left. For more information, refer to this Knowledge Base article. |
| CVE-2024-1086 | N/A | N/A | Not vulnerable. The LoadMaster kernel is not built with, and does not include, the nf_tables component that is required to exploit this potential vulnerability. |
| CVE-2024-1019 | modsecurity | N/A | Not vulnerable. The ModSecurity implementation on LoadMaster does not use the internal resource that is open to this vulnerability. |
| CVE-2024-0962 | libcoap | N/A | Not vulnerable. The vulnerable library is not present on LoadMaster. Any applications running on Real |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | Servers behind LoadMaster that employ this library should be patched using a vendor-supplied update to close this vulnerability. |
| CVE-2024-0727 | openssl | TBD | Limited vulnerability. This issue with the PKCS12 (PFX) certificate file format affects all versions of OpenSSL used in the non-FIPS system in current and previous releases -- with the exception of the OpenSSL 3 FIPS module introduced in LMOS 7.2.54.7.<br><br>The vulnerability exposure on LoadMaster is limited to the action of adding or updating a TLS certificate in the PKCS12 format that was obtained from an untrusted source. In this case, a certificate from an untrusted source could contain NULL arguments that could lead to a process crash; this in turn could be leveraged to mount a denial of service attack.<br><br>LoadMaster is *not* vulnerable to this issue during other certificate operations, because certificates are not stored on LoadMaster in PKCS12 format.<br><br>OpenSSL has not yet made available a release that addresses this issue, as it is viewed as a low severity exploit. When OpenSSL makes such releases available, we will schedule an update for future LoadMaster General Availability (GA) and Long Term Support Feature (LTSF) releases. |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2023-51767 | OpenSSH | N/A | Not vulnerable. This vulnerability requires shell access to the **ssh** client, which is not provided on LoadMaster. SSH login only provides a restricted menu-based interface which cannot be leveraged to exploit this vulnerability. |
| CVE-2023-51385 | OpenSSH | N/A | Not vulnerable. This vulnerability requires shell access to the **ssh** client, which is not provided on LoadMaster. SSH login only provides a restricted menu-based interface which cannot be leveraged to exploit this vulnerability. Exploiting this vulnerability also requires use of the 'ProxyCommand' configuration variable, which is not supported. |
| CVE-2023-48795 | openssh | N/A | Not vulnerable. The OpenSSH configuration on LoadMaster does not permit negotiation of the ciphers that allow this vulnerability (also known as the Terrapin attack) to be exploited:<br>• ChaCha20-Poly1305<br>• all aes[128\|192\|256]-cbc ciphers<br>Although LoadMaster itself is not vulnerable, if you are using LoadMaster to load balance SSH connections to back-end Real Servers, then it is imperative that you either update your backend Real Servers to a release of OpenSSH that includes a fix for this issue, or you should |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | ensure that the real server SSH configuration will not permit connections to be negotiated using the ciphers noted above. A vulnerability scanner that can be used to determine if a server is vulnerable to this attack can be downloaded here. |
| CVE-2023-44487 | Layer 7 | N/A | Theoretically vulnerable. This is a weakness in the HTTP/2 protocol itself. It is mitigated on LoadMaster by the low HTTP/2 concurrency value used in the implementation and by the fact that HTTP/2 is supported only on the client side of the connection. Also, in HTTP/2 Pass-Through mode, LoadMaster simply passes on the HTTP/2 traffic to the real server, and so is not directly vulnerable to this exploit; however, the Real Servers behind LoadMaster remain vulnerable in this scenario.<br><br>Whether an Application Delivery Controller (ADC) is used or not, it is vital that customers implement mitigations directly on HTTP/2 servers to protect against this DoS exploit. A detailed explanation of how this vulnerability is exploited and can be mitigated can be found here. |
| CVE-2023-38408 | openssh | N/A | Not vulnerable. This exploit depends upon a vulnerability in ssh-agent, which is not supported on LoadMaster. |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2023-36755<br>CVE-2023-36754<br>CVE-2023-36753<br>CVE-2023-36752<br>CVE-2023-36751<br>CVE-2023-36750 | N/A | N/A | Not vulnerable. These vulnerabilities are specific to the Siemens RUGGEDCOM ROX product and are not present on LoadMaster. |
| CVE-2023-36664 | N/A | N/A | Not vulnerable. Ghostscript is a third party application that is not supported on LoadMaster (which is not vulnerable to this exploit). |
| CVE-2023-32254 | kernel | N/A | Not vulnerable. LoadMaster does not support the in-kernel SMB server capability required to exploit this vulnerability. |
| CVE-2023-32233 | kernel | N/A | Not vulnerable. Exploitation of this vulnerability requires an elevated level of privilege that is not available on LoadMaster through the UI or a remote shell. Linux servers located behind LoadMaster remain vulnerable and there is no mitigation for this exploit that can be configured on LoadMaster. All Linux Real Servers should be updated with a vendor fix for the Linux kernel. |
| CVE-2023-29130 | N/A | N/A | This vulnerability is specific to the Siemens SIMATIC product; this issue is therefore not present on LoadMaster. |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2023-28708 | N/A | N/A | Not vulnerable. LoadMaster does not use Tomcat, so the LoadMaster itself is not vulnerable to this exploit.<br><br>Applications running behind LoadMaster that use Tomcat are vulnerable and should be updated with a fixed version of Tomcat. In the meantime, LoadMaster customers can take action to close this vulnerability by adding the Secure attribute to cookies coming from back-end Tomcat Real Servers using LoadMaster's content rules as described here. |
| CVE-2023-28531 | openssh | N/A | Not vulnerable. This issue affects OpenSSH versions 8.9 through 9.3. LMOS versions above 7.2.53 use OpenSSH_8.4p1. |
| CVE-2023-28252 | N/A | N/A | Not vulnerable. This vulnerability is specific to the Windows Common Log File System, which is not supported by LoadMaster. Affected Windows servers behind LoadMaster should be updated with the latest patches from Microsoft. |
| CVE-2023-25948<br><br>CVE-2023-24480<br><br>CVE-2023-25770 | N/A | N/A | Not vulnerable. These vulnerabilities are specific to unspecified Honeywell products and are not present on LoadMaster. |
| CVE-2023-24329 | python | N/A | Not vulnerable. The base LMOS system does not include Python and so is not |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | vulnerable.<br><br>If the Python2.7 add-on package is installed, the vulnerability cannot be exploited because LoadMaster does not implement block lists in Python. |
| CVE-2023-24021 | modsecurity | N/A | Not vulnerable. The version of ModSecurity used on LoadMaster (v2.9.6) is not vulnerable to this issue. |
| CVE-2023-23585<br><br>CVE-2023-24474<br><br>CVE-2023-22435 | N/A | N/A | Not vulnerable. These vulnerabilities are specific to the Honeywell Experion product and are not present on LoadMaster. |
| CVE-2023-23397 | N/A | N/A | Not vulnerable. This is a Microsoft Outlook specific vulnerability and does not apply to LoadMaster. No Web Application Firewall (WAF) rule is available to mitigate the vulnerability for servers behind LoadMaster. Microsoft's mitigation recommendations can be found here. |
| CVE-2023-22809 | N/A | N/A | Not vulnerable. LoadMaster is a closed appliance and does not provide a general purpose login or CLI that would allow the user to execute the 'sudo -e' command. |
| CVE-2023-22374 | N/A | N/A | Not vulnerable. This exploit leverages a defect in iControl |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | SOAP, an open communications API, specifically on Big-IP systems from F5 Networks. LoadMaster does not use or support iControl SOAP. |
| CVE-2023-20900 | vmtoolsd | N/A | Not vulnerable. This is a privilege escalation vulnerability present in the SAML implementation in versions of VMtools below 12.3.0. The **Vmtoolsd** add-on package on LoadMaster does not support SAML authentication and so is not vulnerable to this exploit. |
| CVE-2023-6246 | glibc | N/A | Not vulnerable. The version of glibc used on LoadMaster is not vulnerable to this exploit. |
| CVE-2023-4967<br>CVE-2023-4966 | N/A | N/A | Not vulnerable. These denial of service and sensitive information disclosure vulnerabilities exist only on Citrix Netscaler products and are unrelated to LoadMaster. See this Citrix security bulletin. |
| CVE-2023-5129<br>CVE-2023-4863 | libwebp | N/A | Not vulnerable. The LoadMaster product does not use or include the libwebp library. |
| CVE-2023-3595 | N/A | N/A | Not vulnerable. This exploit is specific to Adobe InCopy, which is not supported on LoadMaster. |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2023-3519<br>CVE-2023-3467<br>CVE-2023-3466 | N/A | N/A | Not vulnerable. These arbitrary code execution, cross-site scripting, and privilege elevation vulnerabilities exist only on Citrix Netscaler products and are unrelated to LoadMaster. |
| CVE-2023-2650 | openssl | N/A | Theoretically vulnerable. For OpenSSL versions on LoadMaster, this vulnerability is considered low severity, and affects *only* the display of objects such as X.509 certificates. This can only be done through the UI and API by an already authenticated user and so is considered unlikely to cause a Denial of Service. |
| CVE-2023-2156 | kernel | N/A | Not vulnerable. The version of the kernel used by LoadMaster is not vulnerable to this exploit related to the RPL protocol (routing protocol for low power / lossy networks). |
| CVE-2023-0401 | openssl | N/A | Not vulnerable. This vulnerability applies to OpenSSL 3.0.0-3.0.7 only, which is not supported on LoadMaster. |
| CVE-2023-0286 | openssl | N/A | Not vulnerable. LoadMaster does not use any code that sets the X509_V_FLAG_CRL_CHECK flag and does not use its own network based CRL facility. |
| CVE-2023-0217 | openssl | N/A | Not vulnerable. This vulnerability applies to OpenSSL 3.0.0-3.0.7 only, which is not supported on LoadMaster. LoadMaster also does not use the EVP_PKEY_public_check() function required to exploit this vulnerability. |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2023-0216 | openssl | N/A | Not vulnerable. This vulnerability applies to OpenSSL 3.0.0-3.0.7 only, which is not supported on LoadMaster. LoadMaster also does not use the PKCS7 functions required to exploit this vulnerability. |
| CVE-2023-0215 | openssl | N/A | Not vulnerable. LoadMaster does not use the API as required to expose this vulnerability. |
| CVE-2022-47938<br>CVE-2022-47939<br>CVE-2022-47940<br>CVE-2022-47941<br>CVE-2022-47942<br>ZDI-22-1681<br>ZDI-22-1687<br>ZDI-22-1688<br>ZDI-22-1689<br>ZDI-22-1690 | N/A | N/A | Not vulnerable. LoadMaster does not support the *ksmbd* binary and so is not vulnerable to this exploit. [Note that Linux servers configured behind LoadMaster remain vulnerable to this exploit and should be updated with the latest Linux kernel patch if they are running a vulnerable kernel release.] |
| CVE-2022-25636 | N/A | N/A | Not vulnerable. This exploit is present in Linux kernel versions 5.4 through 5.6.10, which are not supported on LoadMaster. |
| CVE-2022-41040<br>CVE-2022-41082 | N/A | N/A | Not vulnerable. LoadMaster itself is not vulnerable to these exploits; they are zero day vulnerabilities in Microsoft Exchange 2013, 2016, and 2019. There *are*, however, steps you can take on LoadMaster to protect your |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | Exchange deployment from them. Refer to this Knowledge Base article for more information. |
| CVE-2022-32207 | curl | N/A | Not vulnerable. While LoadMaster includes an affected version of curl in the delivered system, the curl command cannot be executed by users and cannot save data to local files. |
| CVE-2022-22965<br>CVE-2022-22963<br>CVE-2022-22950 | N/A | N/A | Not vulnerable. LoadMaster does not use any components of the Java Spring Framework. [This is also true of the Kemp 360 Central and Vision products.] |
| CVE-2022-21907 | N/A | N/A | Partially Vulnerable. This vulnerability exploits a flaw in the Microsoft Windows Server implementation of HTTP trailer headers which may appear at the end of chunked messages. Because trailer headers are not supported on LoadMaster, non-passthrough Layer 7 services on LoadMaster are not susceptible to exploitation of this vulnerability. For passthrough services, the required remediation is to install the latest updates from Microsoft on all vulnerable servers, or turn off trailer header processing on those servers. |
| CVE-2022-21449 | Oracle Java | N/A | Not vulnerable. This is a |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | SE Libraries | | vulnerability in the Oracle Java SE. A successful exploit of this vulnerability can result in unauthorized creation, deletion, or modification of Java SE accessible data. The Oracle Java SE is not present on LoadMaster, which is therefore not vulnerable to this attack. |
| CVE-2022-20866 | N/A | N/A | Not vulnerable. This vulnerability is specific to custom, closed-source SSH libraries produced by Cisco for specific Cisco product lines as specified in the CVE. |
| CVE-2022-4450 | openssl | None | Partially Vulnerable. This exploit could be leveraged only by an already authenticated administrator who could install specially crafted PEM files on LoadMaster, which could in turn cause some system processes to exit abnormally. |
| CVE-2022-4304 | openssl | None | Theoretically vulnerable. An attacker would need to be able to capture traffic between LoadMaster and both the client and real server to get a complete dialogue; and then be able to replay a large number of similar dialogues to recover the plaintext used in a TLS session. By the time this is done, the TLS session is not likely to exist. |
| CVE-2022-3786 | N/A | N/A | Not vulnerable. These CVEs |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2022-3602 | | | describe two high-severity vulnerabilities in OpenSSL version 3.0.6. LoadMaster does not yet support OpenSSL 3 -- running version 1.1.1n as of the date that these vulnerabilities were announced -- and so is not vulnerable to these exploits. Also see this security announcement. |
| CVE-2022-2068<br>CVE-2022-1292 | openssl | N/A | Not vulnerable. LMOS does include an affected OpenSSL release (1.1.1 thru 1.1.n), but the c_rehash script, on which these exploits depend, is not used by LoadMaster. |
| CVE-2022-0847 | kernel | N/A | Not vulnerable. This exploit affects specific versions of the Linux kernel only and LMOS does not use any of the vulnerable kernel versions. |
| CVE-2022-0778 | openssl | 7.2.56.2<br>7.2.54.4<br>7.2.48.7 | LoadMaster is vulnerable to this exploit. The updates listed at left were released on 25 April 2022 to close this vulnerability by upgrading to the OpenSSL release where this issue is addressed (OpenSSL 1.1.1n). For upgrade guidance, refer to the following section: CVE-2022-0778: Upgrade Guidance. |
| CVE-2021-45080 | N/A | 7.2.54.3 | It was possible for a malicious, already authenticated, privileged user to obtain unrestricted access to the Virtual LoadMaster |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | (VLM) disk image and thereby obtain a debug password to the running system. This vulnerability has been closed. |
| CVE-2021-44228 | N/A | N/A | Not vulnerable. The LoadMaster and GEO products are not vulnerable to this exploit, because Java is not used by either product. [Note that the Kemp 360 Central and Kemp 360 Vision products also do not use Java.] |
| CVE-2021-41823 | N/A | N/A | LoadMaster is vulnerable to this medium-level exploit. Customers can add a custom rule to the WAF engine to block it. For further details, refer to the following article: Custom Rule for CVE-2021-41823. |
| CVE-2021-41617 | openssh | N/A | Not vulnerable. This exploit depends on two optional configuration options being set on the target device, neither of which can be enabled on LoadMaster. |
| CVE-2021-41069 | N/A | 7.2.55.0 | Validation has been enhanced for the upload of a Virtual Service template to the system to close a security vulnerability wherein a carefully constructed file can be uploaded as a template and create unwanted files on the filesystem. |
| CVE-2021-41068 | N/A | 7.2.55.0 | The system console has been |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | updated to close vulnerabilities present in previous releases that could allow an already authenticated user to obtain a privileged shell. |
| CVE-2021-36368 | N/A | N/A | Under investigation. The CVE specifically states that to exploit this vulnerability, “an attacker has silently modified the server to support the None authentication option”. So, the attacker would already have to possess admin credentials for the LoadMaster -- at which point there is nothing any system could do to prevent them from modifying security sensitive options. This exploit is also disputed by the vendor: "this is not an authentication bypass, since nothing is being bypassed." |
| CVE-2021-33910 | N/A | N/A | Not vulnerable. This requires the ability to install a kernel module and other programs onto the target system, which is not possible on LMOS. |
| CVE-2021-33909 | N/A | N/A | Not vulnerable. The systemd program is not present on LMOS. |
| CVE-2021-27876 | N/A | N/A | Not vulnerable. LoadMaster does not support the Veritas Backup Agent. |
| CVE-2021-26855 | N/A | N/A | Not vulnerable. Exchange servers behind LoadMaster |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | are still vulnerable to this (and related) attacks as described by this Microsoft blog. See this LoadMaster Knowledge Base article for instructions on how to configure LoadMaster to help protect vulnerable servers until they are patched. |
| CVE-2021-4034 | N/A | N/A | Not vulnerable. This exploit leverages the *pkexec* utility, which does not exist on LoadMaster. |
| CVE-2021-3711 | openssl | N/A | Not vulnerable. The SM2 ciphers that are the subject of this vulnerability are not supported on any release of LoadMaster. |
| CVE-2021-3450 | openssl | N/A | Not vulnerable. This vulnerability affects OpenSSL version 1.1.1h through 1.1.1j, none of which are supported on any release of LMOS. LMOS 7.2.55 supports OpenSSL 1.1.1k, which closes this vulnerability. |
| CVE-2021-3449 | openssl | LMOS 7.2.55.0<br><br>openssl 1.1.1k | An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the *signature_algorithms* extension (where it was present in the initial ClientHello), but includes a *signature_algorithms_cert* extension, then a NULL |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration).<br><br>In LMOS 7.2.55, OpenSSL is updated to version 1.1.1k which addresses this issue. Refer to the following Knowledge Base article for further details: CVE-2021-3449 NULL pointer deref in signature_algorithms processing.<br><br>Also note that in LMOS 7.2.55, the default setting for SSL Renegotiation is now *disabled*. |
| CVE-2021-3156 | sudoedit command | N/A | Not vulnerable. The sudoedit program is not present on LMOS. |
| CVE-2021-1732 | Windows NETLOGON | N/A | Not vulnerable. This is a Windows-only issue and does not apply to Linux-based systems like LMOS. |
| CVE-2020-15778 | N/A | N/A | Not vulnerable. LoadMaster currently runs OpenSSH version 8.4p1; this exploit occurs in 8.3p1 and earlier releases. |
| CVE-2020-15598 | ModSecurity v3 | N/A | Not vulnerable. LMOS uses the ModSecurity v2.9 release line |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2020-14145 | openssh | 8.4p1 | Theoretically vulnerable.<br><br>This is a medium level (5.9) “information leak” issue that could allow unauthorized users to obtain sensitive information during algorithm negotiation. This is not in itself an attack on the system; but, the information obtained could theoretically be used to mount a separate attack that leverages the leaked information. SSH on LoadMaster is not for general purpose login and best practices include locating the management endpoint for the LoadMaster on a dedicated network where only trusted personnel have access, which will mitigate this exploit. |
| CVE-2020-10029 | Glibc | N/A | Not vulnerable. |
| CVE-2020-8515 | N/A | N/A | Not vulnerable. |
| CVE-2020-1967 | N/A | N/A | Not vulnerable. |
| PD-13899 | N/A | N/A | Vulnerability concerning Access Control Lists (ACLs) and Real Servers. Real Servers located on networks *on which LoadMaster also has an IP address* are *always* allowed to access Virtual Services that also have an IP address on that network interface *regardless of all access control list (ACL) settings on LoadMaster*. For Layer 7 services, this issue can be worked around using Content Rules. The |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | workaround for other services is to block access for local Real Servers (if desired) on another network device (firewall, switch, router, and so on). |
| CVE-2019-16905 | openssh | 7.7,7.9<br>8.x-8.1 | Not vulnerable. The vulnerable experimental code is not built as part of LMOS. |
| CVE-2019-0190 | openssh | 1.1.1 | Not vulnerable. Relevant only to Apache servers. |
| CVE-2019-1551 | openssh | 1.1.1 | Not vulnerable. This exploit requires a 512-bit random key and the default for LMOS is 2K. |
| CVE-2019-1549 | openssh | 1.1.1 | Not vulnerable. |
| CVE-2019-1563 | openssh | 1.1.1 | Not vulnerable. LMOS does not support PKCS7 or CMS and it always uses a certificate. |
| CVE-2019-1547 | openssh | 1.1.1 | Not vulnerable. LMOS only uses the libssl interface, which is indicated to be not vulnerable. |
| CVE-2018-15919 | openssh | N/A | Not vulnerable. This issue affects OpenSSH versions 7.8 and below. LMOS versions above 7.2.53 use OpenSSH_8.4p1. |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| CVE-2016-20012 | N/A | N/A | Not vulnerable. SSH access on LoadMaster is only for local console and xroot access; no security relevant information is leaked to a malicious user using the methods described in the CVE. |
| CVE-2014-3356 | openssh | N/A | Not vulnerable. This applies specifically to SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products. All currently supported versions of LMOS run with versions of OpenSSL that contain a fix for this issue. |
| CVE-2013-4786 | IPMI hardware | N/A | Vulnerable. This is a known issue of the IPMI protocol and affects hardware appliances from many vendors. The advice from the IPMI/BMC vendor is to locate the BMC IP address on a secure, internal network that is accessible by trusted personnel only and to use strong passwords on all BMC user logins. It is also possible to disable login to the BMC so that IPMI cannot be used to send commands to the BMC, closing this vulnerability. |
| CVE-2013-4037 | IPMI hardware | N/A | Not vulnerable. This issue applies only to specific hardware listed in the advisory and does not affect LoadMaster. |
| CVE-2013-3587 | Layer 7 | N/A | Vulnerable. This is a |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | vulnerability in HTTP compression that is not specific to LoadMaster, as documented here. Vulnerable websites typically serve dynamic web pages that also carry secret tokens that can be guessed by an attacker over repeated accesses. Best practices include, in order of effectiveness: disabling compression entirely, enabling compression only for static webpages, configuring rate limits for compressed web pages that contain secret data, and continuous log monitoring for repeated failed accesses (indicating possible attempts by attackers to guess secrets). |
| CVE-2011-3389 | N/A | N/A | Not vulnerable. This exploit applies to the "SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products…". This does not apply to LoadMaster. |
| CVE-2011-1473 | openssl | 1.x | By default, LoadMaster is not vulnerable to this exploit because renegotiation is disabled by default in 7.2.55 and above. With renegotiation on, LoadMaster is no more vulnerable than any other network appliance running OpenSSL 1.1.1. This CVE is listed as *disputed*, per this note: "It can also be argued that it is the responsibility of server deployments, not a |

| CVE Entry/Internal ID | Affected Modules | Fixed Version | Comments |
|---|---|---|---|
| | | | security library, to prevent or limit renegotiation when it is inappropriate within a specific environment". Therefore, if you enable renegotiation on LoadMaster, you need to configure your back-end servers properly to limit renegotiation. |
| CVE-2011-5094 | openssl | 1.x | Not vulnerable. Mozilla NSS is not supported on LoadMaster. |
| CVE-2009-2410 | sssd | N/A | Not vulnerable. The sssd utility is not supported on LoadMaster. |
| CVE-2003-0001 | N/A | N/A | Not vulnerable. This exploit affects the Linux kernel version 2.x.x release series; LoadMaster currently (LMOS 7.2.57) runs with the 4.14.137 kernel. |
| CVE-1999-0511 | N/A | N/A | IP forwarding is enabled on LoadMaster by default. IP forwarding can be disabled by enabling the **Packet Routing Filter**, as explained in this Knowledge Base article. |
| CVE-2023-51384 | N/A | N/A | Not vulnerable |

# 2

# CVE-2022-0778: Upgrade Guidance

Refer to your currently running release in the left column below and follow the action listed in the right column to close this vulnerability.

| If you are currently running: | Take the following action: |
|---|---|
| 7.2.56.2 or later | No action necessary. |
| 7.2.55.x / 7.2.56.0 / 7.2.56.1 | Update to 7.2.56.2 (or later). |
| 7.2.54.4 through 7.2.54.x | No action necessary. |
| 7.2.49.x through 7.2.54.3 | Update to 7.2.54.4 (or 7.2.56.2 or later). |
| 7.2.48.7 through 7.2.48.x | No action necessary. |
| 7.2.48.6 or earlier | Update to 7.2.48.7 (or 7.2.54.4 or 7.2.56.2 or later). |