SECURITY NOTICE

SN 2023-03-16 #01: MOD_PROXY SSRF IN LENELS2 NETBOX SUITE - (CVE-2021-40438)

This article contains:

It applies to:

NetBox, NetBox Global, VRx, NetVR, Converged NetBox/VR, NetBox/VRx, Quatro

Executive Summary

Honeywell is aware of the vulnerability “mod_proxy SSRF” in Apache HTTP Server affecting the LenelS2 NetBox Suite.

This vulnerability “mod_proxy SSRF” is published as a CWE-918: Server-Side Request Forgery (SSRF) and affects Apache HTTP Server versions 2.4.48 and earlier. This issue has been assigned CVE-2021-40438 and rated with a severity of Critical. Honeywell strongly recommends that users upgrade to the version identified below to resolve the vulnerability.

Vulnerability Synopsis

1. mod_proxy SSRF in LenelS2 NetBox Suite – (CVE-2021-40438)

   A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

   CVSS Base Score: 9.0 Critical

   CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

   CVE Number: CVE-2021-40438

   https://nvd.nist.gov/vuln/detail/cve-2021-40438

Technical Summary

See https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-40438

Affected Products

Products	CVE	Advisory/Update
NetBox, NetVR v5.4.5 & v5.6.0 *(Including converged NetBox/VR, NetBox/VRx, & Quatro)*	**CVE-2021-40438**	**Upgrade to v5.4.6 or v5.6.0.316**
NetBox Global v3.1.2	**CVE-2021-40438**	**Upgrade to v3.1.3** *(Contact Tech Support for assistance)*
VRx v5.5.2	**CVE-2021-40438**	**Upgrade to v5.5.2**

Remediation

LenelS2 has prepared updates for each affected version of its platforms remediating the vulnerability contained in Apache HTTP Server. These updates may be found in LenelS2 Support Central.

Honeywell strongly recommends that users upgrade to these updated versions as soon as possible.

Customers using earlier unsupported versions of LenelS2 platforms not listed above should verify their Ubuntu version. If Ubuntu 16 UPG3 is used, customers should upgrade to the latest LenelS2 version.

LenelS2 is rapidly working to determine if any additional offerings may be impacted by the Apache HTTP Server mod_proxy SSRF vulnerability. Should we determine that any of our offerings were impacted, additional information regarding mitigations or other actions in response to this matter will follow as our investigation unfolds. More information about the vulnerability is provided by the Apache HTTP Servier Project:

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.49

References

- https://nvd.nist.gov/vuln/detail/cve-2021-40438
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-40438
- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.49

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS, INCLUDING WITHOUT LIMITATION, RECOMMENDED PATCHES OR UPDATES TO ANY SOFTWARE OR DEVICE, SHALL BE AT CUSTOMER'S SOLE RISK AND EXPENSE. CUSTOMER SHALL TAKE ALL APPROPRIATE ACTIONS TO SECURE AND SAFEGUARD ITS SYSTEMS AND DATA. HONEYWELL SHALL HAVE NO LIABILITY FOR (I) CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS OR (II) CUSTOMER'S FAILURE TO SECURE AND **SAFEGUARD ITS SYSTEMS AND DATA. SUCH FAILURES CAN VOID HONEYWELL'S WARRANTY OBLIGATIONS.**
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.