Security Advisory

Multiple vulnerabilities in Nexo cordless nutrunner

1 Advisory Information

Advisory ID: BOSCH-SA-711465

CVE Numbers and CVSS v3.1 Scores:

- CVE-2023-48242
  - Base Score: 6.5 (Medium)
- CVE-2023-48243
  - Base Score: 8.1 (High)
- CVE-2023-48244
  - Base Score: 5.3 (Medium)
- CVE-2023-48245
  - Base Score: 6.5 (Medium)
- CVE-2023-48246
  - Base Score: 6.5 (Medium)
- CVE-2023-48247
  - Base Score: 5.3 (Medium)
- CVE-2023-48248
  - Base Score: 5.5 (Medium)
- CVE-2023-48249
  - Base Score: 6.5 (Medium)
- CVE-2023-48250
  - Base Score: 8.1 (High)
- CVE-2023-48251
  - Base Score: 8.1 (High)
- CVE-2023-48252
  - Base Score: 8.8 (High)
- CVE-2023-48253
  - Base Score: 8.8 (High)
- CVE-2023-48254
  - Base Score: 5.3 (Medium)
- CVE-2023-48255
  - Base Score: 6.3 (Medium)
- CVE-2023-48256
  - Base Score: 5.3 (Medium)
- CVE-2023-48257
  - Base Score: 7.8 (High)
- CVE-2023-48258
  - Base Score: 5.5 (Medium)
- CVE-2023-48259
  - Base Score: 5.3 (Medium)
- CVE-2023-48260
  - Base Score: 5.3 (Medium)

Copyright © 2024 Bosch Rexroth AG

- CVE-2023-48261
  - Base Score: 5.3 (Medium)
- CVE-2023-48262
  - Base Score: 8.1 (High)
- CVE-2023-48263
  - Base Score: 8.1 (High)
- CVE-2023-48264
  - Base Score: 8.1 (High)
- CVE-2023-48265
  - Base Score: 8.1 (High)
- CVE-2023-48266
  - Base Score: 8.1 (High)

Published: 09 Jan 2024
Last Updated: 29 Jan 2024

2 Summary

The Nexo cordless nutrunner running NEXO-OS V1500-SP2 has some vulnerabilities which allows an attacker:

- to read/upload/download/delete arbitrary files in all paths of the system,
- to inject and execute arbitrary client-side script code, arbitrary HTTP response headers or manipulate HTTP response bodies inside a victim's session,
- to authenticate to the web application with high privileges or SSH service with root privileges through multiple hidden hard-coded accounts,
- to read or update arbitrary content of the authentication or results database,
- to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE),
- to upload a malicious file to the SD card containing arbitrary client-side script code and obtain its execution inside a victim's session,
- to access sensitive data inside exported packages or obtain up to Remote Code Execution (RCE) with root privileges on the device,
- to send malicious network requests containing arbitrary client-side script code and obtain its execution inside a victim's session,
- to perform actions exceeding their authorized access.

3 Affected Products

- Nexo cordless nutrunner NXA011S-36V (*0608842011*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXA011S-36V-B (*0608842012*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXA015S-36V (*0608842001*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXA015S-36V-B (*0608842006*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXA030S-36V (*0608842002*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXA030S-36V-B (*0608842007*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXA050S-36V (*0608842003*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2

Copyright © 2024 Bosch Rexroth AG

- Nexo cordless nutrunner NXA050S-36V-B (*0608842008*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXA065S-36V (*0608842013*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXA065S-36V-B (*0608842014*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXP012QD-36V (*0608842005*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXP012QD-36V-B (*0608842010*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXV012T-36V (*0608842015*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo cordless nutrunner NXV012T-36V-B (*0608842016*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo special cordless nutrunner (*0608PE2301*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo special cordless nutrunner (*0608PE2272*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo special cordless nutrunner (*0608PE2666*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo special cordless nutrunner (*0608PE2514*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo special cordless nutrunner (*0608PE2515*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2
- Nexo special cordless nutrunner (*0608PE2673*)
  NEXO-OS V1000-Release <= NEXO-OS V1500-SP2

4 Solution

An updated firmware version is available with fixes of CVE-2023-48243, CVE-2023-48245, CVE-2023-48246, CVE-2023-48247, CVE-2023-48250, CVE-2023-48251, CVE-2023-48252, CVE-2023-48253, CVE-2023-48259, CVE-2023-48260, CVE-2023-48261, CVE-2023-48262, CVE-2023-48263, CVE-2023-48264, CVE-2023-48265 and CVE-2023-48266.

The **Nexo - Firmware V1.500 Service Pack 3** can be downloaded on the platform for sales support and partner communication **myRexroth** or contact your sales partner for instructions on how to retrieve the update. Users are strongly advised to upgrade to the new version.

5 Mitigation

Fixing CVE-2023-48257 would lead to incompatibility of files that have already been exported. Users shall ensure that the file storage is appropriately protected.

5.1 Compensatory measures

Risk mitigating measures are strongly advised. Please define such measures individually depending on your operational environment. In this context, it is strongly advised to operate affected Nexo cordless nutrunner(s) in protected network segments only.

Copyright © 2024 Bosch Rexroth AG

6 Vulnerability Details

6.1 CVE-2023-48242

CVE description: The vulnerability allows an authenticated remote attacker to download arbitrary files in all paths of the system under the context of the application OS user (“root”) via a crafted HTTP request.

- Problem Type:
  - CWE-22 Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 6.5 (Medium)

6.2 CVE-2023-48243

CVE description: The vulnerability allows a remote attacker to upload arbitrary files in all paths of the system under the context of the application OS user (“root”) via a crafted HTTP request. By abusing this vulnerability, it is possible to obtain remote code execution (RCE) with root privileges on the device.

- Problem Type:
  - CWE-22 Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
  - Base Score: 8.1 (High)

6.3 CVE-2023-48244

CVE description: The vulnerability allows a remote attacker to inject and execute arbitrary client-side script code inside a victim’s session via a crafted URL or HTTP request.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
  - Base Score: 5.3 (Medium)

6.4 CVE-2023-48245

CVE description: The vulnerability allows an unauthenticated remote attacker to upload arbitrary files under the context of the application OS user (“root”) via a crafted HTTP request.

- Problem Type:
  - CWE-862 Missing Authorization
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
  - Base Score: 6.5 (Medium)

6.5 CVE-2023-48246

CVE description: The vulnerability allows a remote attacker to download arbitrary files in all paths of the system under the context of the application OS user (“root”) via a crafted HTTP request.

- Problem Type:
  - CWE-22 Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 6.5 (Medium)

Copyright © 2024 Bosch Rexroth AG

6.6 CVE-2023-48247

CVE description: The vulnerability allows an unauthenticated remote attacker to read arbitrary files under the context of the application OS user (“root”) via a crafted HTTP request.

- Problem Type:
  - CWE-862 Missing Authorization
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 5.3 (Medium)

6.7 CVE-2023-48248

CVE description: The vulnerability allows an authenticated remote attacker to upload a malicious file to the SD card containing arbitrary client-side script code and obtain its execution inside a victim’s session via a crafted URL, HTTP request, or simply by waiting for the victim to view the poisoned file.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L
  - Base Score: 5.5 (Medium)

CVE-2023-48249

CVE description: The vulnerability allows an authenticated remote attacker to list arbitrary folders in all paths of the system under the context of the application OS user (“root”) via a crafted HTTP request.

By abusing this vulnerability, it is possible to steal session cookies of other active users.

- Problem Type:
  - CWE-22 Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 6.5 (Medium)

6.8 CVE-2023-48250

CVE description: The vulnerability allows a remote attacker to authenticate to the web application with high privileges through multiple hidden hard-coded accounts.

- Problem Type:
  - CWE-798 Use of Hard-coded Credentials
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

6.9 CVE-2023-48251

CVE description: The vulnerability allows a remote attacker to authenticate to the SSH service with root privileges through a hidden hard-coded account.

- Problem Type:
  - CWE-798 Use of Hard-coded Credentials
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

Copyright © 2024 Bosch Rexroth AG

6.10 CVE-2023-48252

CVE description: The vulnerability allows an authenticated remote attacker to perform actions exceeding their authorized access via crafted HTTP requests.

- Problem Type:
  - CWE-285 Improper Authorization
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

6.11 CVE-2023-48253

CVE description: The vulnerability allows a remote authenticated attacker to read or update arbitrary content of the authentication database via a crafted HTTP request. By abusing this vulnerability it is possible to exfiltrate other users' password hashes or update them with arbitrary values and access their accounts.

- Problem Type:
  - CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

CVE-2023-48254

CVE description: The vulnerability allows a remote attacker to inject and execute arbitrary client-side script code inside a victim's session via a crafted URL or HTTP request.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
  - Base Score: 5.3 (Medium)

6.12 CVE-2023-48255

CVE description: The vulnerability allows an unauthenticated remote attacker to send malicious network requests containing arbitrary client-side script code and obtain its execution inside a victim's session via a crafted URL, HTTP request, or simply by waiting for the victim to view the poisoned log.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
  - Base Score: 6.3 (Medium)

6.13 CVE-2023-48256

CVE description: The vulnerability allows a remote attacker to inject arbitrary HTTP response headers or manipulate HTTP response bodies inside a victim's session via a crafted URL or HTTP request.

- Problem Type:
  - CWE-113 Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
  - Base Score: 5.3 (Medium)

Copyright © 2024 Bosch Rexroth AG

6.14 CVE-2023-48257

CVE description: The vulnerability allows a remote attacker to access sensitive data inside exported packages or obtain up to Remote Code Execution (RCE) with root privileges on the device. The vulnerability can be exploited directly by authenticated users, via crafted HTTP requests, or indirectly by unauthenticated users, by accessing already-exported backup packages, or crafting an import package and inducing an authenticated victim into sending the HTTP upload request.

- Problem Type:
  - CWE-1391: Use of Weak Credentials
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 7.8 (High)

6.15 CVE-2023-48258

CVE description: The vulnerability allows a remote attacker to delete arbitrary files on the file system via a crafted URL or HTTP request through a victim's session.

- Problem Type:
  - CWE-352 Cross-Site Request Forgery (CSRF)
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
  - Base Score: 5.5 (Medium)

6.16 CVE-2023-48259

CVE description: The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.

- Problem Type:
  - CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 5.3 (Medium)

6.17 CVE-2023-48260

CVE description: The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.

- Problem Type:
  - CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 5.3 (Medium)

6.18 CVE-2023-48261

CVE description: The vulnerability allows a remote unauthenticated attacker to read arbitrary content of the results database via a crafted HTTP request.

- Problem Type:
  - CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 5.3 (Medium)

Copyright © 2024 Bosch Rexroth AG

6.19 CVE-2023-48262

CVE description: The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.

- Problem Type:
  - CWE-121 Stack-based Buffer Overflow
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

6.20 CVE-2023-48263

CVE description: The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.

- Problem Type:
  - CWE-122 Heap-based Buffer Overflow
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

6.21 CVE-2023-48264

CVE description: The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.

- Problem Type:
  - CWE-121 Stack-based Buffer Overflow
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

6.22 CVE-2023-48265

CVE description: The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.

- Problem Type:
  - CWE-121 Stack-based Buffer Overflow
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

6.23 CVE-2023-48266

CVE description: The vulnerability allows an unauthenticated remote attacker to perform a Denial-of-Service (DoS) attack or, possibly, obtain Remote Code Execution (RCE) via a crafted network request.

- Problem Type:
  - CWE-121 Stack-based Buffer Overflow
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

Copyright © 2024 Bosch Rexroth AG

7 Remarks

7.1 Acknowledgement

The vulnerability has been uncovered and disclosed responsibly by **Andrea Palanca** from **Nozomi Networks**. We thank him for making a responsible disclosure with us.

8 Revision History

29 Jan 2024: Update as patch is available
09 Jan 2024: Initial Publication

Copyright © 2024 Bosch Rexroth AG