KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

# KRONES Security Advisory “Security vulnerabilities in UltraVNC (March 2019)” (KSA-2019-1)

In March 2019, the cyber security company Kaspersky Lab published more than 20 security advisories regarding UltraVNC. UltraVNC is software used for remote administration of Microsoft Windows systems. The security vulnerabilities described by Kaspersky were initially rated “high” and “critical”, and likely affect all UltraVNC versions so far. An attacker, who successfully exploits server-side vulnerabilities, can likely control vulnerable UltraVNC servers completely. However, there are no exploits available to the best of our knowledge.

**For the affected products and services, Krones rates the likelihood of being exploited as medium. Therefore, timely action is recommended.**

## Affected products and services

The following table lists affected products or services, and specific remediation. Krones recommends implementing the suggested remediation measures.

| No. | Likelihood of exploitation[1] | Affected products or services | Default state and remediation |
|---|---|---|---|
| 1 | Medium | SitePilot<br>• MES 7.*/8.*/9.*/10.*<br>• Former SitePilot versions (LMS, LDS, KAM) | Install patches provided by UltraVNC as there are no known issues regarding compatibility (please be aware that required system restarts might lead to gaps in data acquisition). However, as operation of IT systems is not within the scope of responsibility of Krones/Syskron, we cannot guarantee that the system will operate flawlessly after updating UltraVNC. |
| 2 | Medium | PCS systems (BOTEC) | Krones offers security updates for UltraVNC. Please get in touch with Krones LCS. |
| 3 | Medium | HMI systems based on Windows Embedded Standard 7 with image version:<br>• IDC 4.xx<br>• IPQ 6.xx<br>• INS 1.xx<br>• IRS 1.xx<br>• SAM 1.xx<br>• PGA 4.xx<br>• PGD 1.xx | Krones offers security updates for UltraVNC on https://shop.krones.com/shop/vncpatch. Please check this website.<br>Please get in touch with Krones LCS if you have any questions. |
| 4 | Medium | HMI systems based on Windows XP Embedded, Windows Embedded Standard 2009, or Windows | Krones offers customer-specific solutions. Please get in touch with Krones LCS. |

[1] The likelihood of exploitation is rated by Krones for the default Krones use case of the product in its delivery condition. This value may vary in case of customer-specific solutions or changes of the delivery condition.

| | | | |
|---|---|---|---|
| | | Embedded Standard 7 (if not mentioned in 3). | |
| 5 | Medium | DART based on Windows XP Embedded and software version:<br>• 5.x | Krones offers a new image (5.09.05a). Please get in touch with Krones LCS. |
| 6 | Medium | DART based on Windows XP Embedded and software version:<br>• 4.x | Krones offers customer-specific solutions. Please get in touch with Krones LCS. |
| 7 | Medium | IRIS (using iPanel touch display, and APC620/APC810) based on Windows XP Embedded (FIONA) | Krones offers a new image. Please get in touch with Krones LCS. |
| 8 | None | HMI systems based on Windows 10 | These systems are already patched. |

## Workarounds and mitigations

The following specific workarounds and mitigations are recommended in addition to the remediation measures listed above to further reduce the risk originating from the security vulnerabilities:

- Only use UltraVNC (and other VNC/RFB software) over VPN connections. This is normally the case for UltraVNC at Krones.

## Security contact

If you have any questions regarding this security advisory or other security-related questions, please contact the Product Security Incident Response Team (PSIRT) of Krones: cyber.security@krones.com

OpenPGP key for confidential messages:
https://www.krones.com/ext/securitytxt/cyber.security@krones.com.asc

## Appendix A: Technical description of the vulnerabilities

This section describes each vulnerability in detail. The CVSS v3.0 base score is the current severity rating according to the National Vulnerability Database (NIST) and does not necessarily reflect the actual severity in the default Krones environment.

### Client vulnerabilities

The following security vulnerabilities affect the client-side code of UltraVNC. Therefore, these vulnerabilities are only relevant to clients used to connect to UltraVNC servers (as installed on Krones machinery).

#### Vulnerability CVE-2018-15361

A buffer underflow vulnerability in the UltraVNC client could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

#### Vulnerability CVE-2019-8258

A heap buffer overflow vulnerability in the UltraVNC client could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

## Vulnerability CVE-2019-8259

Multiple memory leaks in the UltraVNC client allow attackers to read stack memory. If combined with other vulnerabilities, it can be used to bypass ASLR (address space layout randomization). Furthermore, it could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 9.3 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).

## Vulnerability CVE-2019-8260

A multiplication overflow in the RRE decoder of the UltraVNC client results in an out-of-bounds read vulnerability that could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

## Vulnerability CVE-2019-8261

A multiplication overflow in the CoRRE decoder of the UltraVNC client results in an out-of-bounds read vulnerability that could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

## Vulnerability CVE-2019-8262

Multiple heap buffer overflows in the Ultra decoder of the UltraVNC client could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

## Vulnerability CVE-2019-8280

An out-of-bounds access vulnerability in the RAW decoder of the UltraVNC client could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

## Vulnerability CVE-2019-8263

A stack-based buffer overflow vulnerability in the ShowConnInfo routine of the UltraVNC client results in Denial of Service (DoS). User interaction is required. The attack could be exploitable over the network.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

## Vulnerability CVE-2019-8264

An out-of-bounds access vulnerability in the Ultra2 decoder of the UltraVNC client could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2019-8265

Multiple out-of-bounds access vulnerabilities connected with the SETPIXELS macro in the UltraVNC could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2019-8266

Multiple out-of-bounds access vulnerabilities connected with the ClientConnection::Copybuffer function in the UltraVNC could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2019-8267

An out-of-bounds read vulnerability in the TextChat module of the VNC client results in Denial of Service (DoS). The attack could be exploitable over the network.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

### Vulnerability CVE-2019-8268

Multiple off-by-one vulnerabilities connected with the ClientConnection::ReadString function in the UltraVNC client could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2019-8269

A stack-based buffer overflow vulnerability in the FileTransfer module of the UltraVNC client results in Denial of Service (DoS). The attack could be exploitable over the network.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

### Vulnerability CVE-2019-8270

An out-of-bounds read vulnerability in the Ultra decoder of the UltraVNC results in Denial of Service (DoS). The attack could be exploitable over the network.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

## Server vulnerabilities

The following security vulnerabilities affect the server-side code of UltraVNC. Therefore, these vulnerabilities are only relevant to UltraVNC servers (as installed on Krones machinery).

### Vulnerability CVE-2019-8271

A heap buffer overflow vulnerability in the file transfer handler of the UltraVNC server could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2019-8272

Multiple off-by-one vulnerabilities in the UltraVNC server could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2019-8273

A heap buffer overflow vulnerability in the file transfer request handler of the UltraVNC server could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2019-8274

A heap buffer overflow vulnerability in the file transfer offer handler of the UltraVNC server could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2019-8275

Multiple improper null termination vulnerabilities in the UltraVNC server result in out-of-bound data being accessed by the remote client. It could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 9.3 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).

### Vulnerability CVE-2019-8276

A stack-based buffer overflow vulnerability in the file transfer request handler of the UltraVNC server results in Denial of Service (DoS). The attack could be exploitable over the network, and may lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

### Vulnerability CVE-2019-8277

Multiple memory leaks in the UltraVNC server allow attackers to read stack memory. If combined with other vulnerabilities, it can be used to bypass ASLR (address space layout randomization). Furthermore, it could lead to remote execution of arbitrary code.

There are currently no exploits available for this vulnerability to the best of our knowledge.

The CVSS v3.0 base score for the vulnerability is 9.3 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).

## Appendix B: Further information

- Kaspersky Lab CERT advisories - https://ics-cert.kaspersky.com/category/advisories/klcert-advisories/

## Appendix C: Changelog

| Version | Date | Changes |
|---|---|---|
| 1.0 | 2019-10-17 | Initial publication by Krones PSIRT |
| 1.1 | 2019-12-10 | Fixed numbering of the table (5 was missing). Added a link to UltraVNC patch website for some HMI systems (no. 3). Updated information about Windows 10-based HMI systems. |