Applied Risk

Industrial Security Advisory

AR2019014

VISAM Automation Base (VBASE) HMI / SCADA 11.5.0.2 Multiple Vulnerabilities

Author: Gjoko Krstic

Release Date: 06 August, 2019

Copyright notice

Overview

The software suffers from multiple vulnerabilities including: Buffer Overflow, Directory Traversal, Password Protection Security Bypass, Insecure File Permissions, Insecure Storage of Sensitive Information and Cryptographic Key Disclosure.

Affected products

The following versions are affected:

- VBASE Editor 11.5.0.2
- VBASE Web-Remote module

The vulnerability has been discovered and validated in software version 11.5.0.2. Older versions are probably affected too.

Impact

An unauthenticated remote attacker may be able to read the contents of unexpected files and expose sensitive data. If the targeted files are used for a security mechanism, then the attacker is able to bypass that mechanism. Due to insecure permissions, a local user can escalate privileges to system level and execute malicious binaries. There is also a known vulnerable ActiveX component that is vulnerable to a buffer overflow attack that allows the attacker to execute arbitrary code on the targeted system. A weak hashing algorithm is used to store sensitive information that allows a bypass of security mechanisms, including the disclosure of cryptographic key for the web login functionality.

Background

VBASE is the central node for automation projects. With its many interfaces to the control level and superior IT systems, VBASE is used as a multifunctional automation platform in professional industrial and building automation. VBASE includes a modern web interface that provides a universal HMI interface based on HTML5. The VBASE Web-Remote enables the display and control of the automation project with smartphones, tablet PCs and all devices with a compatible browser. The Web-Remote generates the necessary HTML5 pages automatically and can be activated on a project basis.

Vulnerability details

Information Disclosure via Directory Traversal

The application suffers from an unauthenticated file disclosure vulnerability when input passed in the URL is not properly verified before being used to include files. This can be exploited to read arbitrary files from local resources with directory traversal attacks.

Applied Risk has calculated a CVSSv3 score of 7.5 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Insecure File Permissions Privilege Escalation

The application suffers from a privilege escalation vulnerability due to weak or insecure permissions on the entire VBASE directory. This could result in elevation of privileges or malicious effects on the system the next time that a privileged user runs the application.

Applied Risk has calculated a CVSSv3 score of 8.2 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H.

Password Protection Security Bypass

Due to weak hashing algorithm used and the insecure permissions issue, a local attacker can bypass the password-protected mechanism of the program by either simply using brute-force attacks, cracking techniques or overwriting the password hash with their own.

Applied Risk has calculated a CVSSv3 score of 7.1 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N.

Cryptographic Key Disclosure

An unauthenticated attacker can disclose the cryptographic XOR key from the webserver remotely to gain information about the login and the encryption/decryption mechanism used for

authenticating users. This can be exploited to bypass authentication and authorization of the HTML5 HMI web interface.

Applied Risk has calculated a CVSSv3 score of 7.5 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Buffer Overflow

The software ships with a known vulnerable ActiveX component that suffers from a buffer overflow vulnerability. This can be exploited by parsing large number of bytes to the vulnerable parameter resulting in overflowing the buffer of the function and overwriting several registers including the instruction pointer. This allows remote attackers to cause a denial of service and possibly execute arbitrary code.

Applied Risk has calculated a CVSSv3 score of 9.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H.

Mitigation

There is no official fix provided by the vendor, nor has there been any response from the vendor since the 8th July 2019.

References

Vendor website:

https://www.visam.com

Product page:
https://www.visam.com/files/kataloge/en/VBASE-Automation-Platform.pdf
https://www.vbase.net/en/hmi-scada-in-machinery-and-plant-engineering.php
https://www.vbase.net/en/building-management-system.php

CWE-121: Stack-based Buffer Overflow:

https://cwe.mitre.org/data/definitions/428.html

CWE-276: Incorrect Default Permissions:

https://cwe.mitre.org/data/definitions/276.html

CWE-23: Relative Path Traversal:

https://cwe.mitre.org/data/definitions/23.html

CWE-200: Information Exposure:

https://cwe.mitre.org/data/definitions/200.html

CWE-922: Insecure Storage of Sensitive Information:

https://cwe.mitre.org/data/definitions/922.html

Contact details

For any questions related to this report, or to request Applied Risk's vulnerability disclosure policy, please contact Applied Risk Research team at:

Email: research@applied-risk.com

PGP Public Key:

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFOgiBQBCACj+Notofe/liuHuc90yy8GAfFn8YFCsMCo7wQmQRNTT43bZQq2
gQr7FTLtOl6rBkOLm8bDk0YY/CtWsjdLh1jlDrWyfU6yIzfcu4CSpn1+5n1ivNN5
17ri+VtmgF392twiKhy2+MC9O4of+GMyu1hy5pIjwi3qGzdNlAnT7m7U/hNzaIR4
ae7+NuWtEvWWKyp3IEEMKTDV/ZOtRD1tfIR8KeBB7Axa8cJdlotw/Ail9TLVB6kt
a/BlvhM/zgWfbEPadnx6B0u7pdW50bTECAs0VHje8mcheTwTCAJo+de3/DqUA34X
oF9aAZWpZWE7VH0O4Q8ZtfrXPFqR2xF8LHhZABEBAAG0REFwcGxpZWQgUmlzayBS
ZXNlYXJjaCBUZWFtIChubyBwYXNzd29yZCkgPHJlc2VhcmNoQGFwcGxpZWQtcmlz
ay5jb20+iQE+BBMBAgAoBQJToIgUAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgID
AQIeAQIXgAAKCRA6nyA79MpeSay8CACSI4UhAget5Z+qEDmz1fe+9krgmx7wwDnF
ig4AVICU8ppJQoUCB5pP6eIV/DM7i+mu8e9zeGlA82t69yTVIANWx72zPmGn5Ku8
4t79gR8V+99PW+O+1rej+96wfL2v+IuOXOcJkTsheUyQZ8Klwc1U8kTdGZEY+/IZ
c32ZhyJ04/cchVP/Zsj2WQIh84wbqa27bTEyyFBnD8FdQ2R4UDTqwACbLgp82m29
P346s80c15RZIX8wUAu0LcNbWJJHRsX6Sa+MozTNug9yWdpZt+nmHEMl95lJYktR
w3+gwyaXeUxALX8Baq2EJDdNx9OlsryiNFdnE9vKIM0+24fTDoqguQENBFOgiBQB
CACtSAm5oBD4kJJY+rtHh6xoytOzP6bFEnrVjqXrXCj+ECG6+N6Droqd072X5hki
qoL1viI4NV+2jrYTtMIu+/nc4zuUFUDRYSm0X/K3WgsqaLA4jdedTm45Tau/Fn6W
26tB5AaddcoDdx6JVGIxFvwU+41KoZ7ouDZo7UEBZ7getPubyR4aPepUsjYnPOUL
0SHH76+b/pC5AZm4crpqWf7Q+qaYQdBIhJbgm5ijFzCyHusYgVGBT1hak81QGpM0
1K9wXki/fJrRyEsWWUjpVSEPRizsFJ60v+NrX50gvvXed8MlX0O9efwgeCmGIVDL
oxF/AmnznYWy0LYWAhh/dW7dABEBAAGJASUEGAECAA8FAlOgiBQCGwwFCQlmAYAA
CgkQOp8gO/TKXkmgdQf/ZtwhL2bs+mlmTUmlT3XO4ekVPRLQKtBYfr8y4rdfnq7Y
MdFYEJAt45R+e4I3I7cIJM1/ImncjFng1EpwFItAXVLa1ktiO6BqT6wBqL6pSBe3
2x5VP8OEnnRubCgYaTotNfiEErgh8cG92tW/TiQArU2dnBcVwYHVwPm450pEv9Aq
BBzgeZ25I1Cv0vlQkQLy9PuTA6DWoxeIxbaMD8ZpKGi+XDrfguJ3tERQMlUA6Fc+
OBkT/NKz8mgecVrwCWbCmScyEhh6onTkevI+mydvsxYG8rE6YVxl3oK5Xi6tvAt9
cUPKKK363nkA1AEoMvTz1bCbmTGvTNWLifoMNtNnGA==
=pAvd

-----END PGP PUBLIC KEY BLOCK-----