eSOMS Third-Party Vulnerabilities - Telerik

CVE-2019-19790

CVE-2019-18935

CVE-2017-11357

CVE-2017-11317

CVE-2017-9248

CVE-2014-2217

CVE-2014-4958

Notice

Affected Products and versions

All versions of eSOMS prior to 6.3.

Vulnerability ID

HAPG ID: 2020-018-PG-eSOMS Telerik

Summary

eSOMS versions prior to 6.3 use a version of Telerik software that is affected by multiple publicly reported vulnerabilities.

An attacker who is able to get access to a vulnerable version of eSOMS may be able to upload malicious files to the server, discover sensitive information, or execute arbitrary code.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVEID	CVSS Score	NVD summary link
CVE-2019-19790	9.8/Critical	https://nvd.nist.gov/vuln/detail/CVE-2019-19790
CVE-2019-18935	9.8/Critical	https://nvd.nist.gov/vuln/detail/CVE-2019-18935
CVE-2017-11357	9.8/Critical	https://nvd.nist.gov/vuln/detail/CVE-2017-11357
CVE-2017-11317	9.8/Critical	https://nvd.nist.gov/vuln/detail/CVE-2017-11317
CVE-2017-9248	9.8/Critical	https://nvd.nist.gov/vuln/detail/CVE-2017-9248
CVE-2014-2217	7.5/Medium	https://nvd.nist.gov/vuln/detail/CVE-2014-2217
CVE-2014-4958	4.3/Medium	https://nvd.nist.gov/vuln/detail/CVE-2014-4958

Link to all issues:

https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Telerik+UI+Ajax&search_type=all

Vulnerability Details

Several publicly reported vulnerabilities exist in Telerik UI for ASP.NET AJAX included in all eSOMS versions prior to 6.3. An attacker could exploit these vulnerabilities to upload malicious files to the server, discover sensitive information, or execute arbitrary code.

Recommended immediate actions

The problem is corrected in the following product versions:

eSOMS version 6.3

Hitachi ABB Power Grids recommends that customers apply the update as soon as possible.

Mitigation Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include ensuring applications and servers are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that must be evaluated case by case. Sensitive application servers should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses be-fore they are connected to a control system.

Workarounds

No workarounds have been identified.

Frequently Asked Questions

What is the scope of the vulnerability?

Several functions used in Telerik UI for ASP.NET AJAX including RadAsyncUpload.

What causes the vulnerability?

The vulnerabilities are caused by deficiencies in third party software used in eSOMS.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could upload malicious files to the server, discover sensitive information, or execute arbitrary code.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, either by connecting to the network directly or through an incorrectly configured or compromised firewall. An attack may also gain access by installing malicious software on a system node or otherwise infecting the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have access to the network hosting the eSOMS application.

What does the update do?

eSOMS version 6.3 includes an updated version of Telerik software that mitigates the reported issues.

When this security advisory was issued, had these vulnerabilities been publicly disclosed?

Yes, these vulnerabilities have been publicly disclosed.

When this security advisory was issued, had Hitachi ABB Power Grids received any reports that this vulnerability was being exploited?

No, Hitachi ABB Power Grids had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Support

For additional information and support please contact your product provider or Hitachi ABB Power Grids service organization. For contact information, see https://www.hitachiabb-powergrids.com/contact-us/ for Hitachi ABB Power Grids contact-centers.