REVISION: A
PUBLICATION DATE: 2022-06-14
DOC. IDENTIFIER: 8DBD000108
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

ActBar2.ocx Vulnerability in Hitachi Energy's PROMOD IV Product

CVE-2010-3591

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of public reports of a vulnerability in the Actbar2.ocx module that affects the PROMOD IV product, versions listed below. An update is available that resolves a publicly reported vulnerability.

An attacker who successfully exploited this vulnerability could delete arbitrary files once the system is compromised.

Affected Products and Versions

List of affected products and product versions:

- PROMOD IV version 11.2, 11.3, 11.4

Vulnerability ID, Severity and Details

The vulnerability's severity assessment is performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the final vulnerability severity score, is not provided in this advisory as it reflects the potential impact of the vulnerability in the customer organizations' computing environment. Customers are recommended to analyze the impact of the vulnerability in their environment and calculate the CVSS Environmental Score.

Vulnerability ID	Detail Description
CVE-2010-3591 CVSS v3.1 Base Score: 9.3 High CVSS v3.1 Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C Link to NVD: click here	A vulnerability exists in the Actbar2.ocx module included in the product versions listed above. The insecure method "SaveLayoutChanges" in the 'Actbar2.ocx' ActiveX controls can be exploited to overwrite arbitrary files. There is the ability for remote attackers to delete arbitrary files once the system is compromised.

Recommended Immediate Actions

The Table below shows the affected version and the recommended immediate actions.

Affected Version	Recommended Actions
PROMOD IV version 11.2, 11.3, 11.4	As file "Actbar2.ocx" is no longer used by PROMOD IV, the file can be safely removed. Navigate to C:\Windows\SysWOW64\ Find the file Actbar2.ocx Delete the file
PROMOD IV version later than 11.4	Install PROMOD IV version11.5 when available – remediation is currently under development

Hitachi Energy recommends that customers apply the update at the earliest convenience. The update removes the vulnerability by removing the vulnerable component.

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 that process control systems 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 have to be evaluated case by case. It is recommended that the PROMOD IV should be deployed inside the customers DMZ/Network. Process control systems 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 before they are connected to a control system.

Additional recommendation is to follow the hardening guidelines published by “The Center for Internet Security (CIS)” https://www.cisecurity.org/about-us/ to protect the host Operating System.

Frequently Asked Questions

What is the affected product, PROMOD IV?

Product IV is software that helps with energy planning, transmission congestion, and price forecasting.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could remove data from the local system or perform modifications in the workflow, that could impact the overall answer/decision on what to do related to the Energy System.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by first obtaining access to the terminal on which PROMOD IV is installed. Next, it needs to try to call the vulnerable function “SaveLayoutChanges” from the ActiveX component. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

The vulnerability is not bound to a network stack. In order to exploit this vulnerability an attacker would need to have physical access to an affected system node, or to construct a HTML page of which a victim on PROMOD IV terminal can click and call the vulnerable “SaveLayoutChanges” function.

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

Yes, this vulnerability has been publicly disclosed by the developer of the Actbar2.ocx.

When this security advisory was issued, had Hitachi Energy received any report that this vulnerability was being exploited?

While an exploit to the CVE-2010-3591 is available [1], Hitachi Energy does not have information to indicate Hitachi's Energy's products have been exploited.

References

1. Oracle Document Capture - Actbar2.ocx Insecure Method, https://www.exploit-db.com/exploits/16053

Support

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy's Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

For additional information and support please contact your product provider or Hitachi Energy service organization. For contact information, see https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2022-06-14	A	Initial public release.