

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

02/06/2015

SUBJECT:

Multiple Vulnerabilities in Ektron's Web Content Management System Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Ektron's Enterprise Web Content Management System that can lead to remote code execution. Ektron's Content Management System is an ASP based content manager used to create, deploy and manage personalized websites. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the content management system. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, and bypass security restrictions.

THREAT INTELLIGENCE

At this time CIS is not aware of this vulnerability being used in the wild.

SYSTEMS AFFECTED:

- Ektron CMS Versions 8.5, 8.7, and 9.1.

RISK:

Government:

- Small government entities: **High**
- Large and medium government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:

Two vulnerabilities have been discovered in Ektron's Content Management System which could lead to remote code execution.

Improper Restriction of XML External Entity Reference (CVE-2015-0923):

This vulnerability is found in the 'xslt' parameter for the 'ContentBlockEx' method within the '/Workarea/ServerControl/WS.asmx' file. This vulnerability could allow an attacker to read arbitrary files.

Improper Control of Resource Identifiers (CVE-2015-0931):

This vulnerability is due to improper configurations in the XML parser. If an attacker specifies the use of the Saxon XSLT parser when handling XSLT files and attacker can provide a maliciously crated file which could allow the attacker to run arbitrary code with the same permission level as the application.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the content management system, or allowing them to view sensitive information. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, and bypass security restrictions. In addition, failed attacks may cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Verify no unauthorized modifications occurred to the system before installing patches.
- Install updates provided by Ektron immediately after appropriate testing.
- Limit access to the Ektron CMS from public Internet

REFERENCES:

CERT:

<http://www.kb.cert.org/vuls/id/377644>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0923>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0931>

SecurityFocus:

<http://www.securityfocus.com/bid/72515>

<http://www.securityfocus.com/bid/72517>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>