

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

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

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

DATE(S) ISSUED:

07/30/2020

07/31/2020 - UPDATED

SUBJECT:

Multiple Vulnerabilities in GRUB2 Could Allow for Complete System Compromise

OVERVIEW:

Multiple vulnerabilities have been discovered in GRUB2, the most severe of which could allow for complete system compromise. GRUB2 is a popular Linux bootloader that works with UEFI secure boot. A boot loader is a piece of software that is designed to load and hand over control to the operating system when the system is first turned on. UEFI secure boot is a verification method added to the boot up process used to verify binaries loaded during bootup against a list of known trusted binary files. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution and lead to complete compromise of the local system.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Grub2 versions prior to 2.06

RISK:

Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in GRUB2, the most severe of which could allow for complete compromise of the local system. Details of these vulnerabilities are as follows:

- A vulnerability exists when parsing grub.cfg that could allow loading of arbitrary code (CVE-2020-10713)

- A heap-based buffer overflow vulnerability exists that can impact the integrity, confidentiality, and availability of the local machine. (CVE-2020-14308)
- Multiple integer buffer overflow vulnerabilities exist. (CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15707)
- A use-after-free vulnerability exists that could allow for arbitrary code execution (CVE-2020-15706)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution and lead to complete compromise of the local system.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches to vulnerable systems immediately after appropriate testing.
- Enforce password complexity, using NIST Special Publication 800-63B, Appendix A as a reference
- Enforce physical security to prevent unauthorized access to the local machine.

July 31 - UPDATED RECOMMENDATIONS:

The MS-ISAC has been informed that multiple distributions of Linux have experienced problems after patching GRUB2. We strongly recommend testing any patches before applying them to live systems and making backups before going live with any changes.

REFERENCES:

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-10713>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14308>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14309>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14310>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14311>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15706>

Debian:

<https://www.debian.org/security/2020/dsa-4735>

NIST:

<https://pages.nist.gov/800-63-3/sp800-63b.html#appA>

July 31 - UPDATED REFERENCES:

Red Hat:

<https://access.redhat.com/solutions/5272311>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

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